Cancer Research UK Response to the Fundraising Regulator’s consultation on proposed changes to the Code of Fundraising Practice relating to GDPR (“Code”)  
December 2017

Cancer Research UK is the largest fundraising organisation in the UK. We receive no Government funding for our research and our work is therefore only possible thanks to the generosity of our supporters. In 2016/17, we spent £432 million on research in institutes, hospitals and universities across the UK. Our vision is to accelerate progress so that three in four people survive their cancer for 10 years or more by 2034.

We strive for transparency and best practice in all of our fundraising operations, including data governance. We welcome this timely review of the Code, given that the General Data Protection Regulation (GDPR) will be coming into effect from May 2018. We are therefore pleased to have the opportunity to respond to this consultation and would be happy to discuss any of these issues in more depth with the Fundraising Regulator if that would be helpful.

Key points
- We welcome the Fundraising Regulator’s efforts to clarify the Code with regards to the GDPR and see it as a positive step to ensuring compliance across the sector.
- However, we are concerned that GDPR provisions are mirrored in the Code but using slightly different wording – such as “legitimate grounds” in Section 5.2.2., which is similar to the GDPR’s “legitimate interests”. In some instances, this requires charities to go beyond the law. We would appreciate clarification on whether this is the intention and, if so, the justification for this. Our preference would be that this refreshed Code mirrors the ICO and GDPR’s wording as closely as possible, so as to avoid confusion.
- We would welcome the inclusion of examples and case studies in this guidance, to support charities in implementation.

Comments on Annex A

s5.1.2: In addition, organisations MUST keep up to date with and have regard to relevant guidance from the Information Commissioner’s Office. This includes the ICO’s Direct Marketing Guidance, its Fundraising and Regulatory Compliance Conference paper and its GDPR consent guidance.

For further information on this topic, please read the Fundraising Regulator’s guide on Personal information, data and consent.

We welcome the Fundraising Regulator suggesting documents ‘to be aware of and consider’ when we are assessing processing. However, we would ask for clear differentiation between guidance that has been subject to formal consultation and adoption, such as the ICO’s Codes of Practice, as opposed to more interpretative guidance such as the Fundraising Regulator’s own guide to personal information, data and consent.

s5.2.1: Fundraising organisations that process personal information MUST* register with the Information Commissioner’s Office (ICO) unless they are exempt.

Further information on who is required to register and the registration process can be found at https://ico.org.uk/for-organisations/register/”

It is our understanding that once the GDPR comes into force, registration with the ICO will no longer be required (although controllers will still need to pay a fee). We would welcome clarification on this point and whether the Fundraising Regulator will issue a further update once the GDPR has come into force.
S5.2.2: When processing personal data (including publically available personal data) for any purpose, organisations MUST*:

a) have legitimate grounds for collecting, using and retaining the personal data. (Further information on the grounds (or ‘conditions’) for processing can be found in Schedule 2 of the Data Protection Act and in the ICO’s Guide to Data Protection).”
b) not use the personal data in ways that have unjustified adverse effects on the individuals concerned;
c) give individuals clear and accessible information about how they will process their personal data, including who the organisation is; what they are going to do with the individual’s personal information; and (where relevant) who it will be shared with. (Further information on communicating privacy information to individuals can be found in the ICO’s Privacy Notice Code of Practice).
d) only handle personal data in ways that the data subject would reasonably expect; and
e) not do anything unlawful with personal data.

With respect to 5.2.2a, we would recommend using consistent language with the terms within the GDPR, in order to promote understanding. For example, we would recommend replacing ‘legitimate grounds’ with ‘legal basis’.

With respect to 5.2.2b, we would welcome more detail on the requirement to ‘only handle personal data in ways that the data subject would reasonably expect’, since at present this does not take into account any of the legal grounds under which this would not be an issue. For example, if processing is necessary for the performance of a contract or for compliance with a legal obligation, we would not necessarily need to comply with the ‘reasonable expectations’ test.

S5.2.8: Where an organisation holds an individual’s personal data to fulfil a contract or because they have gained their consent, the data MUST* be provided to that individual if they request it. The data MUST* be provided free of charge and in a structured, commonly used format which is openly accessible to software (such as a CSV file).”

We recommend that 5.2.8 be reconsidered as it neither exactly matches the right to portability under GDPR, which only covers processing carried out by automated means, or that of the right to access data which covers all personal data irrespective of the legal basis on which it is processed, but is subject to exemptions. We would suggest that if required, this statement simply requires organisations to respond appropriately to all ‘individual rights requests’ made by data subjects to avoid a confusing conflict with what the law actually requires.

S5.3.1: Organisations MUST NOT* share personal data with any other organisation unless they can evidence that they meet the data processing requirements in Rule 5.2.2 above.”

This provision could be interpreted to mean that organisations would need to hold evidence that they were fully compliant in all respects concerning their handling of all personal data, before they were able to share personal data with a third party without breaching the Code. We would therefore prefer this to read “…meet the data processing requirements in 5.2.2. above in respect of that data”. For the avoidance of confusion, we recommend that it be made clear that this provision applies only to sharing of personal data (i.e. with another controller) rather than using a data processor.

S5.5.3 bj From 25 May 2018: Where an individual’s consent is sought, the consent request MUST*:
b) give granular options to consent separately to different types of processing wherever appropriate.”
The wording here slightly deviates from the GDPR requirements. We therefore think that it would be more appropriate to state that consent “must be requested and obtained for each purpose separately.” Otherwise this is suggesting that we must obtain separate consent for activities such as collecting, storing and deleting data – which is not a GDPR requirement.

5.5.4 b) “5.5.4 From 25 May 2018: If consent has been obtained for Direct Marketing communications, organisations MUST:
b) keep consent under review and refresh it if anything changes.”

The requirement to refresh consent “if anything changes” is ambiguous; we would therefore recommend that it be amended to reflect the principle that consent does not last indefinitely and/or that if the purpose for which the data is being processed changes, that consent is gained afresh.

“Legitimate Interest as a basis for Direct Marketing communications

5.5.6: Where an organisation uses or intends to use the Legitimate Interest condition as a legal basis for Direct Marketing communications by phone or post, the organisation MUST be able to evidence: a) that it is necessary to use this condition as a basis for communicating.

Requiring charities to evidence that it is necessary to rely on legitimate interests to send Direct Marketing is significantly beyond the requirements of GDPR, where – in broad terms - the relevant test is that set out in 5.5.6(c) only. If included at all, we recommend that the wording be changed to require organisations to be able to evidence “a) the rationale for using this condition as a basis for communicating.”

5.5.7: When sending Direct Marketing to individuals on grounds of a legitimate interest, organisations MUST explain how their contact data was obtained, and what their legitimate interest is (ie why the charity thinks that the individual might be interested in its cause or its work).”

As with 5.5.6, GDPR does not require this information (on the legitimate interests relied upon) to be on every marketing communication, so this goes beyond the legislation. Can the Fundraising Regulator clarify if the “explain” they are referring to will be satisfied by inclusion in Privacy Notices as per current ICO guidance.

5.6 Requests from individuals to access their personal data

5.6.1. Where an organisation holds an individual’s personal data to fulfil a contract or because they have gained their consent, the data MUST be provided to that individual on request. The data MUST be provided free of charge and in a structured, commonly used format which is openly accessible to software (such as a CSV file).”

This appears to be a repetition of 5.2.8 and seems to be conflating the right to access with the right to portability.

Annex C comments:

8.2.3 The Telephone Preference Service
The Telephone Preference Service (TPS) and Corporate Telephone Preference Service (CTPS) allows individuals or companies to register their telephone numbers to indicate that they do not wish to receive unsolicited sales and marketing telephone calls.
b) Organisations MUST NOT* make direct marketing calls to Telephone Preference Service (TPS)/Corporate TPS (CTPS)-registered numbers unless the person who registered their address has notified the organisation specifically that they consent to receiving Direct Marketing calls from them."

The Telephone Preference Service allows for registration of telephone numbers not addresses, and does not provide information as to who registered the number. We are therefore unable to link a TPS registered number back to the individual who registered it. We recommend that the suggested wording be amended as follows:

“b) Organisations MUST NOT* make direct marketing calls to Telephone Preference Service (TPS)/Corporate TPS (CTPS)-registered numbers unless the person who registered their address being contacted has notified the organisation specifically that they consent to receiving Direct Marketing calls from them.”

For more information please contact Rose Gray, Senior Policy Adviser at 020 3469 8046 or rose.gray@cancer.org.uk.