GDPR: A briefing for foundations

Questions from the webinar, 15 March 2018

The following questions were asked during the webinar, which unfortunately did not record due to a technical glitch. Below are our responses to the questions. Please note that these responses have not been reviewed by the ICO and do not constitute legal advice; they are simply based on our understanding on the regulation and informal discussions.

Do I need to gain consent to send newsletters if they are only sent internally to people within the organisation?

You can choose consent if you feel it is the most appropriate lawful basis, but you are likely to have another appropriate lawful basis for sending your colleagues your newsletter, such as legitimate interests. What's more, if you're sending information by email, this would fall under the Privacy and Electronic Communications Regulation.

When using IT systems which have been procured through consultants, such as Salesforce, is it the responsibility of the provider of that system to align with GDPR, or ours?

The GDPR introduces a higher degree of responsibility for data processors, i.e. organisations which process data but don't have a say in what it's used for, like Salesforce, MailChimp, Dropbox, etc. These companies will have to be compliant with the GDPR in order to operate in the EU and process EU citizens' data, so it is reasonable to assume they will update their terms of service accordingly. But if you want to show you have thought of the risks, it's worth checking their terms and conditions and making sure you are satisfied.

In general, it will be advisable to update contracts with third party IT suppliers to reflect new GDPR requirements. However in practical terms it would be unreasonable if the ICO expected small organisations to negotiate contracts with global companies such as Microsoft and Google. This is an area which the ICO is still looking at and has not reached a final position.

Does GDPR apply to individual people who apply for a grant on behalf of an organisation? Do they "count" as a person or no?

In theory their email address and other details could be classed as personal data, and must be processed lawfully. If this individual is approaching you, is acting on behalf of an organisation, and has a good reason for doing so, it is likely that there'll be lawful basis for processing their data.

Do I need to get consent from my trustees and other volunteers who serve on my committees?

It depends on why you are processing their data. Relevant lawful bases might be that you have a legal obligation or a contract in place, that you have a legitimate interest in sending them information, or indeed that you choose to rely on their consent to send them your newsletter. For each use of data it'll be up to you to determine the most appropriate and feasible lawful basis.

Will this impact the data sharing platform 360Giving?

The data shared on the platform is largely that of organisations making grants to other organisations, and so falls outside the scope of the GDPR.

How should we deal with references – both those giving the references and those they are commenting on?

As far as we can tell, the ICO has not published an update on how references should be handled under the GDPR. For now, the ICO's resources under the Data Protection Act are the best reference: Guide to data protection // employment, the employment practices code, case stories.

If you hold individuals' emails you previously used for marketing for which you do not have consent, can you send an email to them requesting consent?

If you don't have consent because they opted out, it is best not to contact them. If you don't have it because you were relying on a different lawful basis, such as it being in your legitimate interests to send them marketing by post or because they're a corporate subscriber under PECR, then you might be able to continue doing so on that lawful basis. If you want to start using consent as your lawful basis, you should obtain this consent in line with the GDPR requirements. This might mean contacting the individual via another method that you have lawful basis for doing so, e.g. by phone, in person, by post. The Institute of Fundraising has extensive guidance on the use of consent.

What are the rules regarding making use of data obtained using pre-GDPR consent? Do we need to go back to all individuals (who have applied for grants) to ask if we can continue to use that data as part of the assessment process e.g. to know if they have had a grant of a similar type?

Please refer to the answer above about obtaining consent.

As for the purposes of keeping data, you should make it clear what you are obtaining consent for if that is the lawful basis you are relying on. If they didn't already know that that's what you process their data for, then the individual has a right to be informed and the consent should be updated. The Fundraising Regulator has some interesting case studies about how other charities have obtained consent.

In order to re-affirm consent from grantees, could we email their info@ email and request consent from the individuals we seek to contact? Would this align to GDPR? Would it still be ok to identify those individuals within those info@ emails?

An info@ address would not fall under the scope of the GDPR, so you can continue to send emails there. We haven't seen first-hand this tactic of naming individuals being used before, but some charities are asking the email recipient to circulate the email asking for consent among colleagues.

If we want to share a contact we have made with our subsidiary organisation, is it just a case of asking that person on the phone for their consent to pass this on or does this need to be a written consent?

Consent can be given verbally; it's worth making a note of the consent being given for your records.

I see that Microsoft has emailed to say that if we continue using their products after May then that will be taken as acceptance of their new Terms and Conditions. This does not involve opting in – can we use similar wording to obtain consent for our existing database of contacts?

It will depend what Microsoft have in their terms and conditions and the lawful basis they are using for processing data. It may be that they are using the 'soft opt-in' under PECR, which does not apply to 'non-commercial promotions', e.g. charities. It may also be that Microsoft contacted you as you class as a corporate subscriber under PECR. The best way to find out what they are doing – and therefore whether it is an option for you – is to read their updated privacy notice, where they should outline this sort of decision.

Ours is a family trust, we currently have an email list of all family members. Do I need consent from them all?

It depends why you are processing their data and what the lawful basis is for doing so. If you are sending materials which class as direct marketing by post, you can rely on lawful basis. If you are doing so by email, you may need consent. If you are processing their data for other reasons, such as archiving, historical interest, legal obligations to the trust, etc., there may be other grounds for having this email list. If you don't have a reason for holding their data, it is probably better to erase it.

If third party is obtaining consent to share individuals data with us, do I need to also obtain that consent or just record that the third party has that consent?

You don't need to obtain consent a second time, but you do need to be sure that the consent obtained by the third party is GDPR-compliant and that the individuals are fully aware of what you do with their data and why.