More

What's the fuss about Public Authorities and GDPR?

Who and what is this article for?

This article is for anyone who works in fundraising or supporter relations in organisations in the "public" sector or close to it (e.g. universities, publicly-supported cultural organisations, state schools etc.) It aims to help navigate the considerable uncertainty about whether or not consent will be needed for a wide range of activities following GDPR implementation on 25 May 2018.

I've tried to write this article as clearly as possible, although it does have to include a bit of legalese. It might help to read the piece I wrote on Consent vs Legitimate Interest first.

Grounds for Lawful Processing

You need to know that Article 6 of GDPR establishes six grounds for lawful processing – numbered 6.1.a to 6.1.f. The most relevant are:

6.1.a consent;
6.1.e processing by a public authority;
6.1.f processing in the organisation's legitimate interest.

While discussing the use of the last of these, Recital 47 of GDPR says (read it slowly), *"Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis* [legitimate interest] *should not apply to the processing by public authorities in the performance of their tasks."*

So GDPR says that Public Authorities may not rely on legitimate interest grounds for the performance of their tasks. To unpack this, we need to ask what is a public authority and what are "their tasks"?

But before we do, we need to remind ourselves that Legitimate Interest has been the historic legal basis for most data processing on alumni, supporters, donors and potential donors by universities and national museums, state schools and other publicly funded organisations. It does not require consent, so long as the processing isn't harmful to the data subject, upholds their rights, a privacy notice has been delivered and the processing does not involve sensitive data or electronic marketing. In university terms, we are referring to things like having someone on your database, sending them newsletters, direct marketing fundraising materials etc.

More Partnership Ltd, 31 Exchange Street, Dundee DD1 3DJ
+44 (0)1382 224 730 | info@morepartnership.com
www.morepartnership.com | Registered in Scotland SC 216234

What is a Public Authority?

The government has a list of Public Bodies[i], but other organisations are also defined as Public Authorities for the purpose of the Freedom of Information Act. This includes universities, publicly funded museums, state schools, NHS trusts and other similar bodies, many of whom actively fundraise.

The Information Commissioner has not explained how it will decide what is and what is not a Public Authority, nor has it published any definitive timescale for doing so. Indeed, this may be a matter for secondary legislation and not within ICO's powers. However, since ICO also regulates Freedom of Information, it is distinctly possible that the same definition may be used for GDPR purposes.

What does Recital 47 mean by "their tasks?"

This is not entirely clear. It might mean the things the authority is required to do by statute, or it could mean all the things they do.

Might there be some other lawful basis for processing?

Public authorities may rely on Article 6(e) "*processing* [which] *is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*." So, Her Majesty's Revenue and Customs can rely on this to justify processing your information for the purposes of collecting tax.

One might hope that any organisation deemed to be a public authority could rely on Article 6(e) for all its processes. But, in the case of a university, you would have to argue that as well as recruiting and teaching students and collecting their marks and awarding them degrees, all kinds of important but ancillary activities like fundraising and the exploitation of intellectual property and the running of conference facilities were also tasks carried out in the public interest, or "in the exercise of official authority." That's quite a leap.

So, there is no certainty these important but ancillary functions could be carried out under Article 6(e). Some other ground for processing would be needed.

A glimmer of hope?

One possible solution would be to allow public authorities to use Article 6(e) for their core purposes (e.g. teaching students), and "legitimate interest" or some other ground for non-core purposes (e.g. fundraising). This might seem fanciful, but conversations with staff at ICO and their ICO's draft guidance[ii] on consent seems to suggest this might be possible. On page 16 of the draft guidance, in a section entitled "What are the alternatives to consent?", the document says, "*Public bodies cannot generally rely on 'legitimate interests' under the GDPR, but should be able to consider the 'public task' basis in Article 6(1)(e) instead. However, you will need to be able to justify why the processing is necessary to carry out your functions – in essence, that it is proportionate and there is no less intrusive alternative. And, as always, you will need to ensure you are fair, transparent and accountable. Note that this basis* [Article 6(e) processing] *cannot apply if you are acting for purposes other than your official functions – for example, if you are a hybrid body. In such circumstances, you could still consider 'legitimate interests' as a potential basis, as long as the processing is otherwise lawful.*"

This seems to suggest that core tasks for which the public body is established (i.e. teaching students) would be rendered lawful under Article 6(e). By contrast, non-core functions (such as fundraising) could not be lawful under 6(e) because the organisation is not required to do it by statute.[iii] But the last sentence suggests that tasks which are not core statutory requirements could be lawful under Article 6(f) – legitimate interest.

If this really is the direction of travel, then we need to know what a hybrid body is (referred to in the italicised section above.) A search of GDPR and the Data Protection Act produces no other references to hybrid bodies, but it is an established concept in the world of the Human Rights Act. There it refers to a private organisation carrying out a public function (e.g. a private company running a prison) whereas ICO appears to use it to refer to a public body carrying out a "private" function.[iv]

Three things we need to know – and soon

- We need to know which organisations are actually going to be regarded as public authorities. This is very important because knowing the ground for lawful processing is a key building block for compliance. Indeed, GDPR requires certain grounds to be explicitly stated in privacy notices.
- We need to know whether the "hybrid bodies" model really will be the way in which ICO will regulate the processing of data for non-statutory purposes by public authorities.
- We need to know who, ICO or DCMS or Parliament, will decide the answers to these questions, and when.

What to do in the meantime?

In the absence of any legislative "fix", there is a material risk that consent will be the only ground for lawful processing for almost all activities carried out by a fundraising or Development and Alumni function in a public body. Ironically, this is not a situation faced by much of the charity sector since they are not public authorities.

So, it may be tempting to start seeking consent now in case the hybrid solution outlined above fails to materialise, since it's less than 14 months until GDPR comes into effect, and for organisations with annual mailing cycles, these mailings are coming up soon.

There is a significant difference of opinion on whether this is wise, however. A two-part thought experiment illustrates this quite well.

In part one, suppose I asked you "May I punch you in the face?" If you said "No", I would not punch you, and in the very unlikely event you said "Yes", I suppose I would. But if you didn't answer at all, and I still punched you, you would no doubt ask me what on earth I was doing. In the "null response" third scenario, the trouble is I gave you the illusion of a choice – one which I did not intend to let you exercise. And quite clearly your right not to be punched outweighs my interest in punching you.

Part two has me asking you "Would you like a bunch of freesias?"[v] You might say "Yes" or "No" or not reply. If "Yes", you get freesias and if "No", you don't. And if you don't reply, I shall give them to you anyway. Here, the damage or distress caused to you is materially different even if you don't answer, unless you're allergic to freesias. But I still gave you the impression you had a choice.

The serious point of these scenarios is to illustrate the danger of seeking consent if you are actually intending to continue processing the data on some other ground(s). This is because the act of asking for consent creates an illusion of choice. And if you don't intend to let the person exercise that choice, then ICO warns that the act of seeking consent could be inherently unfair and consequently unlawful. Page 13 of the draft consent guidance says: *"If you would still process the personal data on a different lawful basis even if consent were refused or withdrawn, then seeking consent from the individual is misleading and inherently unfair. It presents the individual with a false choice and only the illusion of control. You should identify the most appropriate lawful basis from the start."*

The trouble is, public authorities do not know at present whether they will have a different lawful basis available to them. But if what we want to do with people's data is benign or a positive thing, like the bunch of freesias, then we don't want to have to rely on Consent when Legitimate Interest would do.

What organisations which may be public authorities really need to say is "*In case we can't rely on legitimate interest once all this is resolved, we'd like to ask you for your consent now because time is running out. But if it turns out in law we don't need your consent, then unless you've actively opted out, we're going to rely on legitimate interest and carry on processing your data*." I can't imagine that would pass the GDPR requirement that privacy notices should be clear and concise.

Action now or action later? Or Action now and no need for action later?

If there is no resolution before 25 May 2018, then seeking consent from as many people as possible, as soon as possible, would turn out to have been very sensible. On the other hand, should it become possible to rely on legitimate interest then having asked for consent for all processing could turn out to have been very restrictive because of the "illusion of control" problem. ICO argues that anyone who hadn't responded might have to be treated in the same way as someone who has cognitively said "no".

Some organisations which are public authorities are planning to ask soon for consent for all their activities, not just TPS-phoning and email marketing. Others are holding on a little longer, hoping for resolution to this question in a way which allows them unambiguously to carry on processing in their legitimate interest.

Managing the risk

This matter should be on institutional Risk Registers at the highest level, with actions to include lobbying for resolution of the uncertainty as soon as possible and contingency plans for consent campaigns should there be no resolution.

Adrian Beney
7 April 2017

---

[i] https://www.gov.uk/government/publications/public-bodies-2016

[ii] https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

[iii] Otherwise a public authority could launch an enormous power grab and do any processing it wanted on the basis that it's a public authority.

[iv] Hybrid bodies are also called "functional public authorities" and it may be that ICO prefers to use the phrase.

[v] I am indebted to Rachel Dyson for her elegant extension of my original scenario.