2017 - ICO Guidance on Consent

The Guidance [1] makes a surprisingly broad distinction between public and private sector organisations, even when they process the same data for the same purposes. This would remove important protections when personal data are processed by the public sector, and does not appear to be required by the General Data Protection Regulation [2] that the Guidance aims to implement.

In discussing the alternatives to consent, page 16 treats "necessary for a public task" (Article 6(1)(e) of the Regulation) and "necessary for legitimate interests" (Article 6(1)(f)) as an equivalent pair – the former "likely to give [] a lawful basis for many if not all of [a public body's] activities", the latter available only "if you are a private-sector organisation". However the two are not equivalent for the person whose data are being processed: the legitimate interests of an organisation must be balanced against "the interests or fundamental rights and freedoms" of the individual, whereas no such balance is required when processing for a public task. For a number of different activities performed by both public and private sector education organisations – from protecting the security of computers, data and networks [3] to federated access management [4] and big data/learning analytics [5] – we have found that this legitimate interests test provides valuable guidance to organisations and protection to individuals.

Furthermore many, probably most, of the data processing activities performed by public sector organisations are done by private sector organisations as well. Both act as employers, provide education, raise funds, protect their premises using CCTV, and so on. Applying different rules to this processing, depending solely on whether or not public money is involved (itself not always a straightforward question), can only create uncertainty and opportunities for accidental or deliberate data protection breaches.

Article 6(1)(f) of the General Data Protection Regulation in fact only prohibits the use of legitimate interests "by public authorities in the performance of their tasks". Article 6(3) requires that those tasks be prescribed by law; such laws may modify the Regulation's normal rules. Where a task requires the state to authorise a particular body to work outside normal data protection rules, prohibiting the use of legitimate interests to expand that authority does indeed protect data subjects.

However Recital 49 makes clear that this does not apply to all activities performed by public bodies: "ensuring network and information security" is declared to be a legitimate interest of "public authorities" along with a wide range of both public and private organisations. Public sector activities that are not prescribed by law – such as employment, physical and digital security – cannot be "tasks" in the sense of the Regulation, so should be entitled to use legitimate interests if that is the most appropriate basis. Where public and private sector bodies perform the same function under the same data protection rules it seems confusing and dangerous to insist they be treated differently.

In the interests of both consistency and protection of data subjects, it seems preferable to limit

the use of the "public task" basis to processing activities, such as tax collection, that involve the state assigning additional powers to particular bodies. For activities that are performed on an equal basis by both public and private sector organisations, the greater protection provided by "legitimate interests" and the other legal justifications should be used.

Links
[1] https://ico.org.uk/about-the-ico/consultations/gdpr-consent-guidance/
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[3] https://community.jisc.ac.uk/blogs/regulatory-developments/article/incident-response-and-gdpr-0
[4] https://community.jisc.ac.uk/blogs/regulatory-developments/article/federated-access-management-and-gdpr
[5] https://community.jisc.ac.uk/blogs/regulatory-developments/article/learning-analytics-updated-model