GDPR & BIDs

On the 25th of May this year the General Data Protection Regulation (GDPR) comes into force. This note is not intended to act as a full briefing on GDPR; for that you should try the Information Commissioner's Office (ICO) website or the GDPR Wikipedia page. There is a really useful checklist for making sure that, as a data controller, you are ready for GDPR here on the ICO website.

Here are the headline ways GDPR affects BIDs:

Lawful Basis

GDPR describes something called 'lawful basis' for processing data and lists six different ones:

1. The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes.
2. Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
3. Processing is necessary for compliance with a **legal obligation** to which the controller is subject.
4. Processing is necessary in order to **protect the vital interests** of the data subject or of another natural person.
5. Processing 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.
6. Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Note that 'processing' includes storage of data, not just sending comms.

All of these lawful bases could apply to BIDs but the most pertinent to this note are 1 and 3. It is our understanding that processing the personal data for voters is covered by the third lawful basis, 'legal obligation', because the BID regulations require you to consult with levy payers and their voters on matters relating to ballot and BID proposals. Note that this lawful basis is not elastic; we don't believe it would cover you for processing the personal data of voters to send them other communications (magazines, e-newsletters etc).

For that you will need 'consent' as a lawful basis. So, to summarise:

- Processing data for voter contacts with the purpose of communicating statutory information about your BID (e.g. Business Plan and ballot papers) - **but only those activities** required of you under the BID regulations - is covered by the lawful basis of 'legal obligation'.
- For processing personal data for most other purposes you will need the lawful basis of 'consent'. That also applies to non-statutory comms to voters.
- Other types of lawful basis may apply to you processing personal data:

  Performance of a contract' may apply to your supply chain.

  'Legitimate interests' and 'protect the vital interests' may apply in sensitive areas around security, e.g. dealing with ASB.

Consent

The definition of consent has been tightened up under GDPR. Consent must be explicit for data collected and the purposes data are used for. Data controllers must be able to prove consent (opt-in) and consent may be withdrawn. So you have to tell people what you are going to do with their data and they have to give you explicit consent, which they can withdraw if they wish at any time.

Right to Erasure

A 'right to be forgotten' was replaced by a more limited right to erasure in the version of the GDPR adopted by the European Parliament in March 2014. If a data subject (a person whose personal data you hold) requests their data be erased from your records, you must do so. This right to erasure doesn't apply if your lawful basis to process their data is 'legal obligation' (i.e. they're a voter contact).

The 12 Steps

A useful document at the ICO website is covers 'the 12 steps to take now'. For BIDs these are:

1. Make sure that your team and your board are aware of GDPR coming and what the likely impact will be.
2. Make a list of the different sources of personal data you hold, where it comes from and who you share it with. Note this is only about personal data, i.e. any information relating to a person who can be directly or indirectly identified in particular by reference to an identifier, including names, ID numbers, location data and online usernames.

3. Review your privacy notices and make changes in time for 25th May 2018.
4. Check that you can service the rights a person has about the personal data you hold about them. For example, how would you respond to an access request from someone asking what data you hold about them? You need to respond within a month under GDPR and you can't charge them for it anymore.
5. Review and document your procedures on handling things like access requests and right to erasure.
6. Identify the lawful basis for all the processing of personal data you carry out in the BID.
7. Review how you seek, record and manage consent. Think about refreshing existing consents if they don't meet GDPR standards, e.g. they were gained from a default opt-in webpage.
8. Most BIDs probably don't process personal data belonging to children, but if you do there are special procedures you will need to check out at the ICO website.
9. Review your procedures on what to do if you suffer a personal data breach. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Review your procedures now, because you won't have time when a breach occurs. Here are some good tips.
10. The ICO is signed up to something called 'Data Protection by Design' which is worth considering if you're designing systems for processing personal data, which could cover anything from BID team contacts lists to using Excel and Access to store personal data.
11. Consider designating someone in the BID team to be the Data Protection Officer (DPO). GDPR doesn't require organisations like BIDs to have a DPO, but it's useful to make sure protecting personal data doesn't slip off the agenda for a BID after 25th May. Their duties are here.
12. No BID operates in more than one EU member state so the 12th step doesn't apply!

Why more data protection law?

The reasons behind GDPR are manifold, but some obvious ones are:

- People are waking up to the fact that their personal data has value and is, well, personal. They want better care taking of that personal data and they want organisations that are careless with it to be punished.
- We're all fed up of receiving e-bulletins we never signed up for, marketing bumf from companies we've never heard of and endless nudges toward things we only briefly considered buying in a moment of weakness. GDPR starts the process of redressing the balance of power between the individual and big business.

- We all need better, purer marketing activities that give us better results from people who actually want to hear from us.

At BIDBase we've been faced with 'both barrels' of GDPR; as a data controller (like everyone else) and as a data processor operating BIDBase for almost 13% of the UK BID industry. We've put in place tools for our (free and premium) users that should make compliance pretty straightforward; between now and the 25th May and beyond we'll be helping BIDs in the UK meet their legal obligations on GDPR.