ToucanTech | Alumni, Development & Careers software

Consent vs Legitimate Interests Flowchart

Are you an organization (data controller) operating within the EU* or that processes the personal data of individuals (data subjects) in the EU?

'Personal data' is any information that personally identifies someone, such as a name, address or ID number

GDPR stipulates that you need a lawful basis for processing personal data

'Processing' includes the collection, recording, storage, editing, use, transmission etc of personal data

6 lawful reasons for a data controller to use someone's data

We have the subject's **consent**	We are fulfilling a **contract**	We have a **legal** obligation	We're acting in the subject's **vital interests**	We're acting in the **public interest**	We're acting in our **legitimate interests**

Appropriate to ask for **consent** if:

- *the individual is free to give it and has a real choice (i.e. you won't go ahead and process their data anyway)*
- *you want to give people upfront control of how their data is used*
- *the subject is 13 yrs+ (in UK – 16yrs in some other EU states)***

If using consent to process personal data, you should ensure it is:

- *freely given*
- *prominent and user-friendly*
- *a positive opt-in (e.g. a tick box to be ticked)*
- *granular and specific, stating the controller, what you'll do with the data and why*
- *easy to withdraw*
- *recorded for evidence*

*Does the processing involve **email marketing** (including fundraising emails)*

Yes

- *When carrying out electronic marketing you need to be careful of using 'legitimate interests' as your legal basis for data processing - as this falls under the scope of a separate piece of legislation – PECR (ePrivacy)*
- *Under PECR, you must not send marketing emails to **individuals** unless they have specifically consented or they are an existing customer ('soft opt-in')*
- *However, it's OK to send unsolicited emails to **businesses** (or government bodies) without explicit consent - as long as they can unsubscribe*

No

Appropriate to use **legitimate interests** if:

- *the processing is not required by law but is of clear benefit to you or others;*
- *there's a limited privacy impact on the individual;*
- *the individual should reasonably expect you to use their data in that way; and*
- *you do not want to bother them with disruptive consent requests when they are unlikely to object to the processing*

If using legitimate interests to process personal data, you should:

- *conduct an LIA/ balancing test (considering factors such as the impact on the data subject, what exactly you are doing with their data, would they be surprised etc?) – and retain this documented analysis*
- *tell your community that you're relying on legitimate interests (e.g. a clear privacy notice)*
- *allow your database to opt out of processing*

**The UK Government has confirmed it will bring GDPR in to UK law irrespective of Brexit*
*** The proposed UK Data Protection Bill sets the UK age for consent at 13 (lower than EU default of 16)*

hello@toucantech.com | www.toucantech.com | +44 (0) 203 189 1774