### DRAFTING A PRIVACY POLICY

#### Decide what to include by working out:

* what personal information you hold;
* what you do with it and what you are planning to do with it;
* what you actually need;
* whether you are collecting the information you need;
* whether you are creating new personal information; and
* whether there are multiple data controllers.

#### If you are relying on consent, you should:

* display it clearly and prominently;
* ask individuals to positively opt-in;
* give them sufficient information to make a choice;
* explain the different ways you will use their information, if you have more than one purpose;
* provide a clear and simple way for them to indicate they agree to different types of processing; and
* include a separate unticked opt-in box for direct marketing.

#### Also consider including:

* the links between different types of data you collect and the purposes that you use each type of data for;
* the consequences of not providing information;
* what you are doing to ensure the security of personal information;
* information about people’s right of access to their data; and
* what you will not do with their data.

#### Further considerations for consent:

* What they are consenting to.
* What purpose you are collecting their consent for and what it is limited to i.e. exactly what you will and will not do with their personal data.
* If sharing info with others then must inform and name (in-so-far-as-possible), who the third party is e.g. legal advisors, funders, marketing company, & how / why you are sharing their data with them. Mention that you have ensured that they have sufficient safeguards in place to protect your data.
* Clear, unambiguous language
* Be displayed clearly and prominently;
* ask individuals to positively opt-in, in line with good practice;
* Give them sufficient information to make a choice & provide a clear and simple way for them to indicate they agree to different types of processing.
* Provide option to withdraw consent
* Should regularly renew & refresh consent, especially if consent given in the past was specifically for a particular activity, and whereby individual may think it unreasonable to contact them again about a separate issue.
* MUST have CONSENT on file for any special category information – likely to impact on monitoring information you collect.
* Consider ‘Just-in-time’ consent (e.g. final pop-up box on website with consent + privacy notice) for particularly high-risk data collection / infringement of rights.
* CONSENT is not the right legal basis for processing any employment data (except for optional benefits).

#### PRIVACY POLICY MUST INCLUDE

Controller must provide privacy notice at the time personal data are obtained (free of charge)

Notice must include:

* Identity and contact details of data controller
* Contact details of data protection officer (where applicable)
* Purposes of intended processing and legal basis (if legitimate interest, provide information)
* Recipient(s) of personal data
* Transfer to third country or international organisation (where applicable)
* Period data will be stored or (if not possible) criteria used to determine period
* Right to request access data, to rectification or erasure, right to restriction of processing, right to data portability
* If consent relied upon, right to withdraw consent at any time
* Right to lodge complaint with ICO
* Whether there is a statutory or contractual requirement
* Any automated decision-making (including profiling)

#### Privacy Policy Best Practice

**Unbundled:** Consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.

**Active opt-in:** Pre-ticked opt-in boxes are invalid – use unticked opt-in boxes or similar active opt-in methods (e.g. a binary choice given equal prominence).

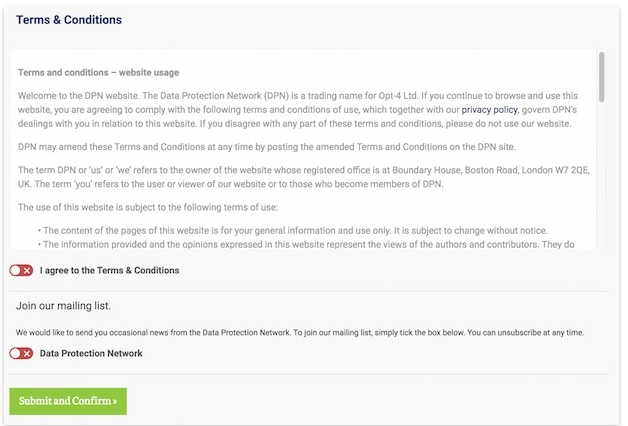
**Granular:** Give granular options to consent separately for different types of processing wherever appropriate.

**Named:** Name your organisation and any third parties who will be relying on consent – even precisely defined categories of third-party organisations will not be acceptable under the GDPR.

**Easy to withdraw:** Tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means you will need to have simple and effective withdrawal mechanisms in place.

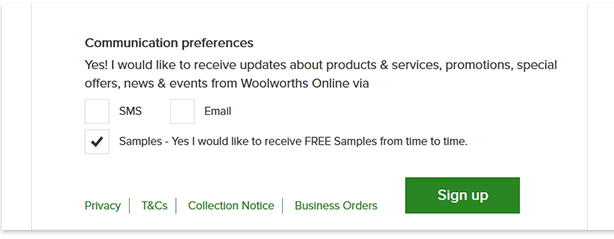
#### Examples

**Unbundled Consent - Data Protection Network**

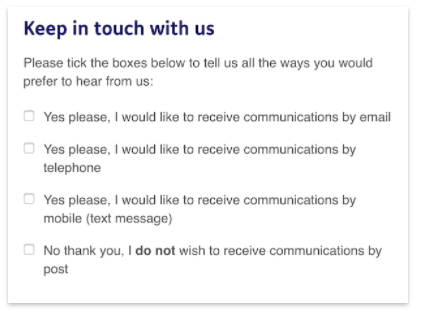


**Granular Consent – Woolworths Australia**

Granular consent means consenting to each contact method separately, which if personalised through data processing falls under the GDPR. It uses three different checkboxes – SMS, email and post (samples). This means users can get comms where they want them, rather than an all-or-nothing approach.



**Age UK**



**Cascading Privacy Notices – Cancer Research**

