

# GDPR Privacy Notice Checklist

## Content Requirements

Does your privacy notice tick all of the following boxes and contain:

- Contact details** for your data protection officer, if applicable;
- The **categories of personal data** that you are collecting (remember this can now include location data, online identifiers, genetic & biometric data);
- Information as to the **sources of the personal data** you collect particularly where you collect personal data from sources other than the individuals;
- Whether the individual must provide the personal data by law, contract, or for another reason, and the **consequences of not providing** the personal data;
- The **purposes for processing** the personal data;
- The **specific legal basis** for each processing activity;
- If your legal basis is **legitimate interests**, either an explanation of those legitimate interests or information as to how individuals can obtain information about those legitimate interests (remember you must undertake a Legitimate Interests Assessment whenever you use legitimate interests as your legal basis for processing);
- The **recipients of personal data**, if any (this section should list specific recipients you share personal data with by name unless it would be unreasonable to do so (e.g. they are likely to change frequently in which case a generic description e.g. payroll administrator will be sufficient);
- Whether you intend to transfer personal data **outside the EEA** and the permitted route you intend to use e.g. the country you're sending the information to has an adequacy decision, you have model contract clauses in place with the entity you're transferring the data to, or an exemption applies;
- What your **retention period** is in relation to each category of personal data processed (this can be done by including a reference to a separate Data Retention Policy;
- Whether you are using **automated decision-making**, including profiling, the auto-decision logic used, and the consequences of this processing for the individual;

- Information about **individuals' rights** in relation to their personal data, including the right to object to or restrict data processing, the right to erasure also known as the right to be forgotten, and the right to data portability;
- Notice of the individual's **right to withdraw consent** (where consent is relied upon as the legal basis for processing); and
- Notice of the individual's **ability to file a complaint** with the local supervisory authority (ordinarily the ICO) and information about how to exercise that right.

## Style and Format Requirements

- Is your Privacy Notice:
  - Concise;
  - Intelligible;
  - In clear, plain and easy to understand language;
- Is your Privacy Notice suitable for the individuals whose personal data you process? Consider whether you process the personal data of children or vulnerable individuals and whether your Privacy Notice should be adapted for them. Do you regularly deal with customers whose first language is not English? Consider translating your Privacy Notice if necessary.
- Is your Privacy Notice easily accessible i.e. can an individual obtain all relevant privacy information within two clicks of your organisation's homepage.
- Do you inform individuals that they can obtain a hardcopy Privacy Notice if they require and tell them how to do so.
- Do you have processes in place to ensure Privacy Notices are delivered to individuals:
  - At the point at which you collect their personal data when you are collecting their personal data directly;
  - At the first communication with them, or within one month of receiving the personal data, when the personal data is obtained from another source.