MILLS & REEVE
Achieve more. Together.

Privacy notice checklist

Under the UK GDPR, individuals have a right to certain information about how their personal data is used.

Each “controller” of the personal data is obliged to provide this information to the relevant individual. Although, there are some situations when you do not need to do this, including where an individual already has the information, or if it would involve a disproportionate effort to provide it.

The information that needs to be provided to individuals is often set out in a privacy notice. If your organisation is controlling what happens with people’s personal data and the UK GDPR applies, use the checklist below to make sure you are providing the right information about what personal data you process, why and how.

Identity of your organisation and contact details Individuals have a right to know the identity of any organisation (or any person) who determines what happens with their personal data, and must be given contact details.	
Contact details for your data protection officer (if applicable) Not all organisations are legally obliged to appoint a data protection officer (DPO), but if you have appointed a DPO, you must provide contact details for them. Under the UK GDPR, you must appoint a DPO if: • You are a public authority or body (except for courts acting in their judicial capacity). • Your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking). • Your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.	
Purpose of the processing You need to tell individuals why you are using their personal data. This should be as specific as possible and generalisations should be avoided.	
Legal basis for processing the personal data There are different bases on which it is lawful to use, or otherwise process, someone’s personal data. Different rights apply, depending on which legal basis is applicable, so you must tell individuals which legal basis you are relying on to use their personal data.	
Categories of personal data concerned (if not collected directly from the individual) If you're not obtaining the personal data directly from the individual data subject, then you need to tell that individual what categories of their personal data you are controlling.	
Source of the personal data (if not collected directly from the individual) If you're not obtaining the personal data directly from the individual data subject, then you need to tell that individual where you've obtained their personal data from, and whether it's a publicly accessible source.	
Recipients or categories of recipients of the personal data (if applicable) Individuals should be told who their personal data will be shared with (if any). For instance, if your organisation will share their personal data with group companies or credit reference agencies, then you need to inform the individual of this.	

Details of any personal data transfer outside the UK or to international organisations (if applicable) Individuals have a right to know if your organisation is transferring their personal data to a country outside the UK or to an international organisation, such as the UN or NATO. In such circumstances, you must also confirm whether or not adequacy regulations cover the transfer, or refer to the appropriate safeguard that has been put in place for the transfer and explain how the individual can obtain a copy of the relevant appropriate safeguard (such as approved standard data protection clauses) or where they have been made available.	
How long you intend to store the personal data You should also list any criteria that you use to determine retention periods for personal data.	
Rights of the data subjects You should ensure that individuals are aware of what rights they have over their own personal data. These include: • Rights to access, rectification, erasure, objection, restriction and data portability (although some of these rights are qualified). • The right to withdraw consent (if consent is the lawful basis for the processing). Details of how individuals can exercise this right should be included in a privacy notice. • The right to make a complaint to a supervisory authority. In the UK this will be the Information Commissioner's Office (ICO). Their contact details should be included in a privacy notice.	
Any statutory or contractual requirement to provide the personal data (where it is collected directly from the individual) Individuals should be told if there is a requirement for the data subject to provide certain personal data – this may be a statutory or contractual requirement. They should also be informed of the implications of failing to provide the relevant personal data.	
Details of any automated decision-making being utilised (if applicable) You should outline the details of any automated decision-making (including profiling) that is being used in relation to personal data collection and processing. In such cases, you need to provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of that processing for the individual.	