Citation

GDPR – 'Privacy notice' checklist

The following are all requirements for creating an effective and GDPR-compliant privacy notice. They are applicable to several situations, such as website privacy notices, fair processing notices and internal information for employees.

Each organisation must review its own data processing activities in order to complete a privacy notice, including identifying the data they process, the legitimate purposes they use that data for, who they share data with and why.

Requirement	✓/✗
Identity and contact details of the Data Controller (in an employment context this is the employer) and if applicable (e.g. global organisations), the Controller's local representative *(e.g. Company name, legal department, e-mail address, telephone number)*	
Contact details of Data Protection Officer, if applicable *(e.g. DPO's name, e-mail address, telephone number)*	
Purposes of processing *(e.g. providing a service; employment of employees; management of customer-related activities such as providing products / services and marketing; management of supplier-related activities such as selecting suppliers)*	
Legal basis of processing *(this must be based on one or more of the lawful grounds set out in Article 6)* *(e.g. data subject consent; performance of a contract; compliance with legal obligation; legitimate interests of the controller)*	
If relying on the "legitimate interest" ground for processing, identify the legitimate interest (*e.g. for the purpose of fraud prevention or in some cases, direct marketing*)	
Identify the recipients or categories of recipients to whom personal data will be disclosed, including any recipients located outside the European Economic Area ("EEA") *(e.g. group companies; third-party service providers; law enforcement / government authorities)*	
Confirm whether the information will be transferred to a third country or recipient outside the EEA and if so, details of the recipient and destination country and the level of protection that will be afforded to the data, by reference to: (*1*) *whether or not the recipient country is covered by a Commission adequacy decision;* ***AND*** (*2*) *details of the safeguards you have in place (if any) to ensure the security of the personal data (e.g. Binding Corporate Rules; standard contractual clauses);* ***OR*** (*3*) *the risks of the transfer due to the absence of an adequacy decision and /or appropriate safeguards (if applicable).*	

Requirement	✓/✗
The envisaged time limits for erasure of different categories of personal data or, if not possible, the criteria used to determine this period *(e.g. 6 years following termination of employer / employee relationship, 1 year following termination of customer relationship)*	
Data subjects' rights: *(1) to request access to and rectification or erasure of their personal data,* *(2) to restrict the processing of their personal data,* *(3) to object to processing (this information must be clearly distinguishable from the other information),* *(4) to object to direct marketing (this information must be **explicitly offered** to the data subject, so that it is clearly distinguishable from other information),* *(5) to data portability (where applicable)*	
Where you are relying on the data subjects consent to process their data, their right to withdraw their consent at any time	
Data subjects' rights to complain to the Information Commissioner's Office (or other supervisory authority if outside the UK) if there is a problem	
Whether the provision of personal data is a statutory or contractual requirement (or necessary to enter into a contract) as well as the possible consequences of failure to provide such data	
Whether providing the data is mandatory or voluntary *(i.e. whether or not it is necessary in order to enter into the contract)*	
The possible consequences of failing to provide that data *(e.g. non-receipt of a benefit)*	
Details of any automated decision making, particularly profiling (where applicable), meaningful details of the logic involved in this processing and the potential consequences of such processing	

The following information should also be included where you have not received the data directly from the data subject (e.g. where obtained from a third party or publicly accessible source)	
Categories of personal data concerned (*e.g. customer data like contact information and purchasing habits, supplier data like contact details and bank account details, special categories of data such as racial or ethnic origin / political opinions or philosophical beliefs / trade-union membership / health information / sex life or sexual orientation information / biometric data which may uniquely identify an individual*)	
Source of the data and (where applicable), whether or not it came from publicly available sources	