Information to be provided in your privacy notice

Information to be provided	When data is obtained directly from data subject	When data is NOT obtained directly from data subject	Guidance
Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer	✔	✔	Identify the controller and DPO and contact details, providing phone, email and postal (as a minimum)
Purpose of the processing and the legal basis for the processing	✔	✔	Ensure each specific purpose is stated together with the relevant Article 6 legal basis (you should state all that apply to each purpose as there may be more than one). Where you are processing special categories of data, the Article 9 conditions should also be identified but you can do this generically. If you are processing criminal convictions/offences data you must state the specific EU/National law that allows you to do this.
The legitimate interests of the controller or third party, where applicable	✔	✔	You should provide details of the legitimate interest assessment (LIA). In practice, this may not be the easiest information to summarise so you could provide a link to the assessment document or state that an individual can obtain further information on the LIA on request, if this information is not contained or linked to the notice.
Categories of personal data		✔	Listing categories of data is only required where the data has not been obtained from the individual directly but it may be helpful to list all the data.
Any recipient or categories of recipient of the personal data	✔	✔	You must provide information on recipients that is meaningful to the individual which generally involve naming all recipients including controllers, joint controllers and processors with whom you share data. If you choose to name only categories of recipients, this should be as specific as possible indicating the type of recipient e.g. controller or processor, the industry, sector and sub-sector and the recipients' location.
Details of transfers to third country and safeguards	✔	✔	The GDPR permits international transfers on a number of ground. You should provide meaningful details on transfers which generally means specifying the country and the corresponding adequacy mechanism and where possible providing links to further information on the specific adequacy mechanism.
Retention period or criteria used to determine the retention period	✔	✔	It is not sufficient to generically state data will be kept as long as necessary for the legitimate purpose. Where relevant, the different retention periods should be stated for each category of personal data and/or different processing purposes, including where appropriate, archiving periods.

Continued...

The existence of each of data subject's rights	✔	✔	This information should include a summary of what the relevant right involves and how the individual can exercise them for your organisation. If there is anything in the UK Data Protection Bill that qualifies or restricts a data subjects' rights, this also needs to be stated. The right to object to processing must be clearly and separately stated at the time of the first communication at the latest.
The right to withdraw consent at any time, where relevant	✔	✔	Need to reference the right to withdraw consent at any time. The mechanism for doing this must use the same interface used to provide consent i.e. if it was provide by an online tick box, the mechanism to withdraw the consent must be equivalent.
The right to lodge a complaint with a supervisory authority	✔	✔	Needs to be clear that this complaint can be about a general breach of the GDPR and that complaints can also be made to the controller/organisation.
The source the personal data originates from and whether it came from publicly accessible sources		✔	Specific sources of the data you process need to be provided unless not possible, although it may be adequate to provide generic descriptions of the source rather than name them e.g. the type of organisation/industry/sector; whether the data is public or privately held and where the information was held (i.e. EU or non-EU).
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✔		For example in an employment context, it may be a contractual requirement to provide certain information to a current or prospective employer. Online forms should clearly identify which fields are "required", which are not, and what will be the consequences of not filling in the required fields.
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✔	✔	This applies to solely automated decisions that have a significant or legal effect on individuals. However, you should be transparent about any profiling you undertake.
Timing	When data is obtained.	Within 1 month of obtaining data or on first communication if obtained for this communicaiton or before disclosure if being shared with another party.	