Information notices

At a glance

- Controllers must provide information notices, to ensure transparency of processing.
- Specified information must be provided, and there is also a general transparency obligation.
- Much of the additional information will not be difficult to supply – although it may be hard for organisations to provide retention periods
- There is an emphasis on clear, concise notices.

To do list

- ☐ Audit existing information notices and review and update them.
- ☐ For data which is collected indirectly, ensure that notice is given at the appropriate time.
- ☐ Work with relevant partners who may collect data on your organisation's behalf to assign responsibility for notice review, update and approval.

Commentary

The principle of *"fair and transparent"* processing means that the controller must provide information to individuals about its processing of their data, unless the individual already has this information. The information to be provided is specified in the GDPR and listed below. The controller may also have to provide additional information if, in the specific circumstances and context, this is necessary for the processing to be fair and transparent.

The information must be provided in a concise, transparent, intelligible and easily accessible way, using clear and plain language (in particular where the data subject is a child).

What must a controller tell individuals?

The GDPR requires more extensive information to be provided than the Data Protection Directive – although much of the additional information is already mandatory in some Member States.

Information which is not specified in the Data Protection Directive is indicated in italics.

- Identity and contact details of the controller (or its representative, for a non-EU established controller); *contact details of the Data Protection Officer*.
- Purposes of processing *and legal basis for processing – including the "legitimate interest" pursued by the controller (or third party) if this is the legal basis.*
- Recipients, or categories of recipients.
- *Details of data transfers outside the EU:*
  - *including how the data will be protected (e.g. the recipient is in an adequate country; Binding Corporate Rules are in place etc.); and*
  - *how the individual can obtain a copy of the BCRs or other safeguards, or where such safeguards have been made available.*
- *The retention period for the data – if not possible, then the criteria used to set this.*
- That the individual has a right to access *and port data, to* rectify, erase *and restrict his or her personal data, to object to processing and, if processing is based on consent, to withdraw consent*.
- *That the individual can complain to a supervisory authority.*
- *Whether there is a statutory or contractual requirement to provide the data and the consequences of not providing the data.*
- If there will be any automated decision taking – together with information about the logic involved and the significance and consequences of the processing for the individual.

When must a controller provide this information?

Controller obtains information directly from individual

- At the time the data are obtained.

The controller must also tell individuals what information is mandatory and the consequences of not providing information.

Controller does not obtain directly

- Within a reasonable period of having obtained the data (max one month); or
- If the data are used to communicate with the individual, at the latest, when the first communication takes place; or
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

The controller must also tell individuals the categories of information and the source(s) of the information, including if it came from publicly accessible sources.

- The controller does not have to provide this information to the individual if it would be impossible or involve a disproportionate effort. In these cases, appropriate measures must be taken to protect individuals' interests and the information notice must be made publicly available.

  There is also no need to provide the information notice:

  - if there is an EU or member state law obligation for the controller to obtain/disclose the information; or
  - if the information must remain confidential, because of professional or statutory secrecy obligations, regulated by EU or Member State law.

If the controller later processes personal data for a new purpose, not covered in the initial notice, then it must provide a new notice covering the new processing.

Providing all of this information is hard to reconcile with the GDPR's own requirement of conciseness and clarity. To help better achieve this, there is an ability for the Commission to introduce standardised icons by means of delegated acts. If introduced, these would then also need to be displayed to individuals.

Where can I find this?

Articles 12-14
Recitals 58, 60, 61 and 62