GDPR Data Processing Notices

A processing notice is a written notice which must be provided to an individual by an organisation which processes personal data relating to that individual as a data controller.

Previously processing notices only had to be fair, but under GDPR they must be transparent and set out extensive information for the relevant individual.

A processing notice is intended to make the individual aware of how their personal data is being used and what personal data relating to them is being processed. Simply holding personal data is classed as processing, so even organisations merely storing data may have to provide a processing notice.

The obligation to provide a processing notice only applies to data controllers. There is no requirement to provide one if you are only a data processor in relation to the relevant personal data. Essentially the difference is that a data controller has control over how data is used and processed, and a data processor only ever processes personal data strictly in accordance with the instructions of a data controller. It is possible to be both a data controller and a data processor in relation to the same personal data, so whether an organisation is a data controller or data processor for any particular processing activity may require careful consideration.

The information required to be provided in a processing notice does not have to be provided if the individual already has it. So where a third party provides the same information, then it may be possible for an organisation to avoid the need to provide a further processing notice. For example a processing notice provided by one party in a supply chain which covers all the activities of the other parties in the supply chain would negate the need for the other parties in the supply chain to provide their own processing notices. There are however risks in relying on the processing notices of third parties, and this issue will require careful consideration.

Reviewing existing data processing notices can be carried out to identify the gaps, however often it is usually simpler to provide a new processing notice which is GDPR compliant rather than try to fill in the blanks not covered by other processing notices.

We have set out two checklists below. These are based on Articles 13 and 14 of GDPR. These requirements come into force on 25th May 2018, though it would be advisable to provide the required processing notice in advance of that date in relation to existing personal data held.

Article 13 covers the requirements for the processing notice where personal data is collected directly from the individual. Article 14 covers the requirements for the processing notice where personal data is collected indirectly, i.e. not directly from the individual but via a third party.

Whilst there is a lot of similarity between the checklists, there are some differences. If personal data relating to an individual is collected both directly and indirectly, which is not unusual, then the processing notice provided to that individual must cover the items in both checklists. To assist with this where items in a checklist are unique to that checklist (i.e. do not appear in the other checklist) then they are included in bold and italics.

It should be noted that processing notices are now quite detailed and long documents which also need to be clear and easy to read. They can be difficult to prepare correctly and you should consider taking legal advice on the drafting of any processing notices. This checklist is not a substitute for legal advice.

It is also difficult to draft a processing notice without the organisation having carried out a full data mapping exercise. Without inputting the information from a data mapping exercise there is considerable risk of a processing notice being incomplete or inaccurate in some respect as it will not cover all the data processing activities. In addition it is prudent to make sure that a processing notice covers future activities which are planned or likely to minimise the need to update and re-issue a revised data processing notice in the future.

If the data controller intends to process data for purposes not included in a previous data processing notice, then the data controller must provide the additional information on that purpose and any additional relevant information required under Articles 13 or 14 of GDPR. This generally means having to update and re-issue a processing notice.

Please note that the requirement to provide a processing notice is a separate legal issue as to whether any consents are required from the individual for any activities which involve the processing of their personal data. Whilst the issue of obtaining consents is often combined with a processing notice, legally they do not need to be combined and could be separated.

DATA PROCESSING NOTICE CONTENTS - GDPR ARTICLE 13

Data collected directly from the individual

At the time when the data controller collects personal data from an individual, at the time of collection the data controller must provide a data processing notice which contains the following:

Part 1

The identity and contact details for the data controller, and where applicable their representative. Representatives are, for example, persons acting as agents for the data controller in the collection of the personal data.

Contact details for the Data Protection Officer if one has been appointed. If one has not been appointed we would generally advise that a data protection contact point is provided, even though not strictly required, but care is taken not to refer to them as a Data Protection Officer and to make it clear that they are just a point of contact for data protection matters.

The purposes for the processing of the personal data and the legal basis for processing. This will require detailed consideration to make sure that all existing and anticipated purposes are covered and the basis which is being relied on for processing the personal data for each of these reasons is clear. The processing notice should therefore link each purpose for processing with the relevant legal basis for processing.

Where the data processing is for the legitimate business interests of the data controller or a third party, the processing notice must state what those legitimate business interests are. This issue will require careful consideration as to what the legitimate interests are, how they are expressed and how they are not overridden by the interests or fundamental rights and freedoms of the individual.

The recipients or categories of recipients of the personal data, e.g. data processors. If categories of recipients are being used (which is generally preferable), then we would advise that as much detail as possible is provided as otherwise there is a risk that requirement of transparency is not met.

If applicable, the fact that the data controller intends to transfer the data to a third country or international organisation and, if so, the basis and safeguards applicable, e.g. adequacy decision by EU Commission, binding corporate rules, adoption of EU Commission Model Clauses, etc. and where the individual can obtain a copy of them.

Part 2

The period for which the data will be stored or if that is not possible the criteria that will be used to determine how long the data is stored for. This may be a mix, so some data may be stored for definite periods time and for other personal data there may be assessment criteria applied which may determine how long it is stored for.

The existence of the right to make a subject access request, or to exercise the right to be forgotten, right to rectification, right to restrict processing, right to object to processing and the right to data portability. If it is clear that any of these will not be applicable then we usually advise that this is flagged here too.

Where processing is based on consent, the right of the individual to withdraw consent at any time. The individual must also be able to withdraw consent as easily as the consent was given in the first place.

The right to make a complaint to the supervisory authority, which in the UK would be the Information Commissioners Office. We would advise that contact details or at least the website address for the ICO is provided.

Whether the provision of the personal data is a statutory or contractual requirement or a requirement necessary to enter into a contract and whether the individual is obliged to provide the personal data and the possible consequences of it not being provided.

The existence of any automated decision making including profiling and meaningful information about the logic involved as well as the significance and the envisaged consequences of the processing for the individual.

DATA PROCESSING NOTICE CONTENTS - GDPR ARTICLE 14

Data not collected directly from the individual

Where the personal data has not come directly from the individual the data controller must provide a data processing notice at the time when the data controller first contacts an individual or within a month of collection of the data at the latest or when the personal data is to be disclosed to a third party (whichever comes first).

Where collection of personal data is both direct and indirect then the first to apply of each of the respective time limits for provision of a processing notice should be used to determine when the processing notice is provided. The processing notice must contain the matters set out below:

Part 1

The identity and contact details for the data controller, and where applicable their representative. Representatives are, for example, persons acting as agents for the data controller in the collection of the personal data.

Contact details for the Data Protection Officer if one has been appointed. If one has not been appointed we would generally advise that a data protection contact point is provided, even though not strictly required, but care is taken not to refer to them as a Data Protection Officer and to make it clear that they are just a point of contact for data protection matters.

The purposes for the processing of the personal data and the legal basis for processing. This will require detailed consideration to make sure that all existing and anticipated purposes are covered and the basis which is being relied on for processing the personal data for each of these reasons is clear. The processing notice should therefore link each purpose for processing with the relevant legal basis for processing.

The categories of personal data concerned. This is so that the individual knows what types of personal data are being processed.

The recipients or categories of recipients of the personal data. If categories of recipients are being used (which is generally preferable), then we would advise that as much detail as possible is provided as otherwise there is a risk that requirement of transparency is not met.

If applicable, the fact that the data controller intends to transfer the data to a third country or international organisation and, if so, the basis and safeguards applicable, e.g. adequacy decision by EU Commission, binding corporate rules, adoption of EU Commission Model Clauses, etc. and where the individual can obtain a copy of them.

Part 2

The period for which the data will be stored or if that is not possible the criteria that will be used to determine how long the data is stored for. This may be a mix, so some data may be stored for definite periods time and for other personal data there may be assessment criteria applied which may determine how long it is stored for.

Where the data processing is for the legitimate business interests of the data controller or a third party, what those legitimate business interests are. This issue will require careful consideration as to what the legitimate interests are, how they are expressed and how they are not overridden by the interests or fundamental rights and freedoms of the individual.

The existence of the right to make a subject access request, or to exercise the right to be forgotten, right to rectification, right to restrict processing, right to object to processing and the right to data portability. If it is clear that any of these will not be applicable then we usually advise that this is flagged here too.

Where processing is based on consent, the right of the individual to withdraw consent at any time. The individual must also be able to withdraw consent as easily as the consent was given in the first place.

The right to make a complaint to the supervisory authority, which in the UK would be the Information Commissioners Office. We would advise that contact details or at least the website address for the ICO is provided.

The source of the personal data and, if applicable, whether it came from a publically available source. This is so that the individual knows where the personal data has come from. It is preferable for each of the personal data categories to be attributable to each source.

The existence of any automated decision making including profiling and meaningful information about the logic involved as well as the significance and the envisaged consequences of the processing for the individual.