Privacy Notices under #GDPR: Have you noticed my notice?

As you all know by now the General Data Protection Regulation (GDPR) is here and it is (as predicted) starting to get various people fired up ready for its 2018 implementation date. (Dear reader, it is still relevant despite the Brexit vote.) We've been exploring various aspects of the GDPR and in this particular blog I want us to look at the concept of privacy notices and what they will need to start looking like under the Regulation.

Data Protection Act 1998:

Under the current Data Protection Act 1998, and indeed the Information Commissioner's Office Privacy Notices Code of Practice, privacy notices should be on any collection point where personal data is being collected from a Data Subject. Especially if being collected for a new purpose. In that notice Data Controllers should (at the very least) include the following;

- The identity of the Organisation in control of the processing;
- The purpose, or purposes, for which the information will be processed; and
- Any further information necessary, in the specific circumstances, to enable the processing in respect of the individual to be 'fair' (in accordance with the 1st Principle).

The requirements also outline that this information must be clear and in 'plain English' and your purposes cannot be too vague. The less vague the purpose the less likely it's going to be a valid consent (or indeed a valid notification if you are not relying on consent).

While privacy notices vary most of them aren't that much longer than your average paragraph (the paragraph I've just written for example) and that, providing it's clear, concise and meets your legal grounds for processing, is generally how privacy notices work under the Data Protection Act 1998. Further information on a Controllers processing is then often outlined in Terms and Conditions either in the contract paperwork or online.

The New World:

The GDPR builds on the current expectations around privacy notices but expands on the requirements based on the widened first principle which now specifically requires controllers to be transparent with their processing.

Article 13 Paragraph 1 (a-f) of the GDPR outlines that the following information should be provided to the data subject at the point of data collection;

(a) *the identity and the contact details of the controller and, where applicable, of the controller's representative;*

(b) *the contact details of the data protection officer, where applicable;*

(c) *the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;*

(d) *where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;*

(e) *the recipients or categories of recipients of the personal data, if any;*

(f) *where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitablesafeguards and the means by which to obtain a copy of them or where they have been made available.*

Depending on what processing is going on, **Article 13 Paragraph 2 (a-f)** states that controllers will also need to provide some of the following;

(a) *the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;*

(b) *the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;*

(c) *where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;*

(d) *the right to lodge a complaint with a supervisory authority;*

(e) *whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;*

(f) *the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*

Now if you are engaging in some quite complicated processing, like in the insurance industry for example, your new notices under GDPR are going to need to strike a balance between being 'too much information' and being far too simple and high level that they don't actually meet your transparency requirements to demonstrate effective notice or consent.

Article 13 Paragraph 3 also outlines that should a controller seek to process personal data for purposes different to which it was collected the controller shall project the subject (prior to that processing commencing) information on that purpose and any other relevant information from paragraph 2.

I've attempted to 'mock up' what one of these new notices could look like. Now this is very much an imaginary one but if we assume that a controller is processing Personal Data for complex purposes their notice may look something like this;

Your Personal Data:

What we need

The A Notice Ltd will be what's known as the 'Controller' of the personal data you provide to us. We only collect basic personal data about you which does not include any special types of information or location based information. This does however include name, address, email etc.

Why we need it

We need to know your basic personal data in order to provide you with notice writing and analysis services in line with this overall contract. We will not collect any personal data from you we do not need in order to provide and oversee this service to you.

What we do with it

All the personal data we process is processed by our staff in the UK however for the purposes of IT hosting and maintenance this information is located on servers within the European Union. No 3rd parties have access to your personal data unless the law allows them to do so.

We have a Data Protection regime in place to oversee the effective and secure processing of your personal data. More information on this framework can be found on our website.

How long we keep it

We are required under UK tax law to keep your basic personal data (name, address, contact details) for a minimum of 6 years after which time it will be destroyed. Your information we use for marketing purposes will be kept with us until you notify us that you no longer wish to receive this information. More information on our retention schedule can be found online.

What we would also like to do with it

We would however like to use your name and email address to inform you of our future offers and similar products. This information is not shared with third purposes and you can unsubscribe at any time via phone, email or our website. Please indicate below if this is something you would like to sign up to.

Please sign me up to receive details about future offers from A Notice Ltd.

What are your rights?

If at any point you believe the information we process on you is incorrect you request to see this information and even have it corrected or deleted. If you wish to raise a complaint on how we have handled your personal data, you can contact our Data Protection Officer who will investigate the matter.

If you are not satisfied with our response or believe we are processing your personal data not in accordance with the law you can complain to the Information Commissioner's Office (ICO).

Our Data Protection Officer is Notice McNoticeface and you can contact them at mypersonaldata@anotice.com.

This example is working on the assumption of a simple data processing arrangement. The more complex your data processing the more complex that notice and consent capture will need to be.

But this must be comprehensible to the average consumer and cannot be a work of 'legal-ee brilliance' that makes no sense to those not trained in law.
I suspect that notices will allow 'outlines of categories' of types of processing and third parties however we shall see how big these categories can be. After all, the bigger the 'bucket' the less you are actually giving a robust 'informed' notice to a data subject.

In addition to all of this, **Article 14** states that should you obtain Personal Data via a means not direct from the Data Subject themselves you also need to provide a notification to them (with some exceptions);

(a) *within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;*

(b) *if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or*

(c) *if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.*

The requirement is to provide them with very similar information that you would provide to them if you collected the data directly. How you do this will be a matter of some discussion to come but excluding the reasons outlined in Article 14 (5) (a – d), if you aren't collecting directly you will now need to take steps to advise and 'notify' the Data Subject of what you are up to.

Now that is quite a long list of things to notify a data subject of, especially if you are delivering various services to the data subject (and collecting data on them) via various means. But Paragraph 4 does say that all of the above shall not apply if the data subject already has the data. So, for example, if a customer is simply renewing a service and nothing about the provision of that service (the processing) has changed then there is no obvious requirement here to re-issue the original notice at that point of renewal.

We will delve into the concept of consent at another time (very soon) but the requirement to be transparent as well as the requirement to ensure you have a clear and documented consent means that privacy notices are going to have to become more than just a long legal document but that far away from what we are doing today (assuming we are doing them correctly that is).

Scott Sammons *CIPP/E, AMIRMS* is an experienced Data Protection & Information Risk practitioner and blogs under the name @privacyminion. He is on the Exam Board for the Act Now Data Protection Practitioner Certificate.