GDPR: THE DATA PROTECTION PRINCIPLES (BUT NOT AS YOU KNOW THEM JIM!)

Having recently attended the Information Commissioner's Office Data Protection Practitioners Conference in Manchester, I should start this blog post by echoing the words of our outgoing Commissioner, Christopher Graham, that the Regulation text is not the final version until later this year when it has been reviewed and fully translated for all 28 member states.

But as the Regulation is unlikely to change in material terms, let's crack on!

Whenever you see blogs and articles about the new EU General Data Protection Regulation, they are often focusing on what's new and "exciting", be that in a good or bad context (see our summary here). But this blog post will look at some of the things that are remaining familiar, albeit in an edited 'reshuffled' form.

So let's go back to basics - the Data Protection Principles. Now under the current Data Protection Act 1998 there are 8 principles that cover things from legitimate purpose to retention and security. Under the Regulation these are changing. Chapter 2, Article 5 (1) (a)-(f) now outlines the principles:

"Personal Data shall be;

1, processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

2, collected for specified, explicit and legitimate purposes and not further processed in a a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes; ('purpose limitation');

3, adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

4, accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

5, kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for *longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 83(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');*

6, processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality');"

Now while the Regulation text doesn't specifically say "principle 1" etc. it does confirm these as the principles and it is logical to assign numbers (as opposed to A,B,C). Principle A just doesn't have the same ring to it as, "the first principle". I suspect that these will now become known by their subject matter, so for example you would have "the accuracy principle" and "the data minimisation principle."

You will notice that we are also down to 6 principles from our current 8 under the DPA. The 2 "missing principles" have been amalgamated in to the new 6 principles. All the current requirements in the 8 principles are still here but they are now outlined in the finer detail of the text. So, for example, principle 6 in the DPA ("processed in accordance with data subjects rights") is not specifically called out as a principle in the Regulation but it is outlined in Ch2 Art 5 (1) (a) that information will be processed in a "fair and transparent manner". The requirements of which, outlined in the rest of the Regulation, require Data Controllers (and indeed processors) to ensure that Data Subjects can exercise their rights as outlined in the text in Chapter 3.

The same applies to the current principle 8 of the DPA 1998 "not transferred to a country outside of the EEA without adequate protections" principle. Because the 'protections' are outlined in other principles (Chapter 4, section 2 (Security) for example) and the regulatory nature of the Regulation, it is expected that as part of your processing under the other principles you will share data internationally in the correct fashion.

As the saying goes, the devil is indeed in the detail with this Regulation. Below I've put the relevant sections into the principles to which they relate. There is some overlap but generally if you're talking about principle 1, then the references are all sections of the text that are relevant to some degree. This list is by no means exhaustive but it does give you a view as to how the principles are intertwined into the detailed text.

Principle:	Relevant Text References	Summary of Requirement:
Lawfulness, fairness and transparency *(Chpt 2, Art 5 1(a))*	**Lawfulness:**	
	Chpt 2 – Art 6 (1-4)	Lawfulness of processing
	Chpt 2 – Art 7 (1-4)	Conditions for consent
	Chpt 2 – Art 8 (1-3)	Conditions for child's consent
	Chpt 2 – Art 9 (1-4)	Processing of special categories of personal data
	Chpt 2 – Art 10	Processing of data relating to criminal convictions
	Chpt 5 - Art 44	General principle for transfers
	Chpt 5 - Art 45 (1-9)	Transfer with an adequacy decision
	Chpt 5 - Art 46 (1-5)	Transfers by way of appropriate safeguards
	Fairness:	
	Chpt 3 Sct 2 Art 13 1a (a-f)	Information to be provided where the data is collected from the data subject
	Chpt 3 Art 14 1-5	Information to be provided where the data has not been obtained from the data subject
	Transparency:	
	Chpt 3 Art 12 1-8	Transparent information, communication and modalities for exercising the rights of the data subject
	Chpt 4 Art 26 1-3	Joint Controllers
	Chpt 4 Art 41 1-6	Monitoring of approved codes of conduct
	Chpt 4 Art 42 1-8	Certification

Principle:	Relevant Text References	Summary of Requirement:
Purpose limitation *(Chpt 2, Art 5 1 (b))*	Chpt 2 – Art 9 (1-4) Chpt 4 - Art 25 1-3 Chpt 4 - Art 35 1 - 11 Chpt 5 - Art 47 2 (b) Chpt 5 - Art 49 1 (a-g) Chpt 9 - Art 88 1-2	Processing of special categories of personal data Data Protection by design & default Data Protection impact assessment Transfers by way of Binding Corporate Rules Derogations for specific situations Processing in the employment context
Data minimisation *(Chpt 2, Art 5 1 (c))*	Chpt 4 Art 25 1-3 Chpt 5 Art 47 2 (d) Chpt 9 Art 89 1	Data Protection by design & default of Binding Corporate Rules Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
Accuracy *(Chpt 2, Art 5 1 (d))*	Chpt 3 Art 18 1-3 Chpt 3 Art 19	Right to restriction of processing Notification obligation regarding rectification, or erasure of personal data or restriction of processing
Storage limitation *(Chpt 2, Art 5 1 (e))*	Chpt 2 – Art 6 3 Chpt 2 – Art 11 (1-2) Chpt 5 Art 47 2 (d) (e)	Lawfulness of processing Processing which does not require identification Binding Corporate Rules
Integrity and confidentiality *(Chpt 2, Art 5 1 (eb))*	Chpt 4, Sct 2- Art 32 (1-4) Chpt 4, Sct 2- Art 33 (1-5) Chpt 4, Sct 2 - Art 34 (1-4) Chpt 4, Sct 3 - Art 35 7	Security of processing Notification of a personal data breach to the supervisory authority Communication of a personal data breach to the data subject Data protection impact assessment

In the next few posts I'll be exploring these principles more and some of the related requirements to see what this means in practice and what further location specific standards we should be on the watch for.

Scott Sammons is an Information Risk and Security Officer in the Medico-Legal Sector and blogs under the name @privacyminion. Scott is on the Exam Board for the Act Now Data Protection Practitioner Certificate.

Read more about the EU Data Protection Regulation and attend our full day workshop.