Why are the 2018 data protection changes important to my business?

Or Don't Panic! – Think

Steven Marc Rhodes

The GDPR – The Law

* It will come into effect before Brexit is concluded (25th May 2018) and will be required for 'equivalency'
* It is a regulation, not a Directive. So it will not become an Act of UK Parliament
* It is a 'code'. It is free standing
* The Principles are substantially the same.

What's changed?

* Data Protection 'by design and default'
* New, compulsory reporting requirements
* Stricter requirements on consent and on certain categories of data (especially medical data)
* The purpose of use of data to be clear
* Right to be forgotten/Portability/Access/Compensation
* Bigger fines

Data Protection – 'by design and default' (Arts 24 & 25)

* The GDPR is concerned about business processes, not technology per se.
* Your systems should only be allowing you to gather information: 1. You need and 2. Clients have consented to.
* A firewall is not enough; no 'bolt on' solution will protect you. Be cautious of false promises.
* You have business recovery procedures, ensure GDPR is filtered into them.
* Integrate, Integrate, Integrate.

Reporting Procedures

* Art 33. Data breaches must be reported to the ICO ‘within 72 hours’ Including:
* the nature of the personal data breach: categories and rough number of data subjects and data record affected;
* the name and contact details of the data protection officer/contact point with further details;
* the likely consequences;
* measures taken/proposed, to address the breach, including mitigation.

Reporting Procedures

* Art 34. You must tell the data subject of the breach 'without delay' unless:

* 34.3 (a) You have the right 'technical and organisational' protection measures, and they were applied to the data affected by the breach, in particular as encryption, etc;
* (b) You have taken subsequent measures to stop it happening;
* (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication.

‘technical and organisational’

* An encryption product is a very good idea!
* Some are out there which can ensure online encrypted access (IT product providers have suitable products)
* BUT you need the procedure to go with the product
* INTEGRATE DP procedures with disaster recovery (who will notify whom of breaches, what happens after that?)

Consent

* Recital 42 “a declaration of consent pre- formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.” (also Art 4.11)
* ‘Data subject’ must:
  * know the identity of the controller and
  * know the purposes of the processing for which the personal data are intended
  * have a genuine or free choice
  * be able to refuse or withdraw consent without detriment.

  Art 32 ‘no pre-ticked boxes’

Medical data

* Art 9.1 "Processing of personal data ...concerning health… *shall be prohibited*." Unless
  * Art 9.2 (a) the data subject has given explicit consent to the processing of those personal data *for one or more specified purposes*. [SMR italics]
  * Do NOT mix marketing and provision of services. Make sure the data-subject/client knows what's happening. Brokers: check no medical details are 'lying around'.

New Elements 1

* Right to be forgotten:
  * You need to be able to wipe details from your system permanently
  * You also need to be prepared to cooperate with others to ensure that any ‘public profile’ of the data subject is deleted
* Portability
  * It’s the data-subjects data, not yours. S/he can do what they like with it (including going to your competitors).

New Elements 2

* Access:
  * Have systems ready to be able to retrieve your data with ease. If the data-subject wants to see everything you hold on them, they can. Your ability to retrieve that data quickly shows your compliance ‘by design and default’.
* Compensation
  * It’s not only fines. You are now more easily liable for misuse of data.

Penalties

* Lesser offences, maximum 2% turnover or EUR 10 million
* Serious offences 4% turnover or EUR 20 million

But these are ‘worldwide’ figures.

As with most fines, the real loss is reputational.

NB: US firms. You won’t necessarily be fined, but your clients will!

Big Firms/Product Providers

* If you have over 250 employees and you haven't appointed a Data Protection Officer, start looking now.
* If you <250 employees and have complex data needs, consider a DPO, or equivalent, anyway
* Talk to your lawyers/consultants/IT contractors
* Start analysing your data flows **now**

Big Firms/Product Providers

* Look at your governance procedures:
* Is GDPR listed on your risk register? If so, how does that relate to your IT operations. Do you have designated people to liaise and plan?
* Does your Chairman know? Is GDPR on agenda of Board Committees (audit/compliance, etc)?
* Are your databases clean and tidy (radiator syndrome)

Small Firms/IFAs

* Appoint someone to look at GDPR e.g. trainee/new consultant:
  * Probably digital native
  * Builds professional expertise
  * Develops a skill set.

  Give them space to concentrate on GDPR (some days home leave to read and understand, etc)

Small Firms/IFAs

* The GDPR is lengthy and thorough, but its principles are not difficult to grasp
* Much of this is stuff that you should have been doing already!
* Most compliance is cultural. Start thinking about it now, and it won't be a shock on 2nd Jan (or 28th May!)

General Principles

* Only gather data you are going to use now
* Do not gather data on a ‘nice to have’ basis (About Schmidt)
* Treat this as an opportunity to de-clutter
* Do not have data ‘lying around’ (whether electronically or in paper files)
* Integrate, Integrate, Integrate (everything is Data)
* DON’T PANIC!

Steven Marc Rhodes

steven@stevenmarcrhodes.com

07801555860