BRIEFING NOTE:

MAPPING YOUR DATA

LEGALLY PRIVILEGED - STRICTLY CONFIDENTIAL

Stephens Scown LLP, Curzon House, Southernhay West, Exeter EX1 1RS
T: 01392 210700 **F:** 01392 274010 **DX:** 8305 Exeter **W:** Stephens-scown.co.uk

Ref: TM/BP/STEP

Please note that this is a complex area of law and that if you attempt the specific processes set out below without advice then you do so at your own risk.

Some key terms used in this briefing note:

Word	Meaning
DPA	Data Protection Act 1998
GDPR	General Data Protection Regulation
PECR	Privacy Electronic Communication Regulation
ICO	The Information Commissioners Office (which enforces the DPA, GDPR and PECR)
Personal Data	Any data that can be used to identify a living individual. Common examples include name, address, email, telephone. There is a second set of data called Sensitive Data which I will not touch on in this email.
Controller	An organisation with collects and stores personal data.
Processor	Any organisation which deals with i.e. "processes" personal data.

What is changing

The GDPR is the new law which comes in to force on 25 May 2018 and will replaced the DPA 1998. I have outlined below some of the key changes between the two laws:

	DPA	GDPR
Maximum Fine	£500,000.	4% of turnover or £20,000,000 – whichever is higher.
Reporting system	ICO required registration for some businesses .	All businesses which handle personal data may be subject to ICO.
Liability	Controller only.	Both Controller and Processor – but it is the Controller's liability to choose the right processor.
Data Collection	Can rely on implied consent to collect and	Explicit and informed consent must be sought at all times except where consent may form part of a legally binding contract

	process data.	for the provision of goods or services and/or there is a PECR exemption.
Personal rights	Individuals have the right to see what data you hold about them for a £10 fee.	Individuals own the data you hold/process and can request sight of, deletion or transfer of that data without charge ("right to inspect/erasure/portability").
ICO powers	Businesses have to register and ICO may ask for inspection.	All businesses can be fined by ICO and when a breach occurs they must report it within 72 hours.
Privacy and security	Should be addressed within processes.	Should be a key driver for an organisation. This is a case of "privacy by design".

The GDPR will apply across the whole of the EU and the UK (regardless of Brexit) is designed to put to focus of data security and treatment on to those who control and/or process it. If you receive personal data from a subject, you will have responsibilities to that data subject – in essence, it is their data, not yours, and you must look after it. This includes not passing that data to third parties without the data subjects' permission.

Data Security

Cybercrime is a type of criminal behaviour that is become increasingly popular and takes multiple forms – financial transactional interference, sexual offences, harassment, libel and commercial espionage, damage and disruption.

Data security is the fundamental element to reducing risk from all types of cybercrime. Ensuring data is secure and treated in accordance with the relevant legal requirements means that if you are a victim of cybercrime then the damage will be mitigated.

Data loss isn't the only risk – there is negative PR and the new fines which are being used to corral businesses into compliance.

With words like "cyber" and "data", the process of being data law compliant and ensuring cybersecurity risk is reduced is often left to the ICT team. Data security should be considered by all managers in an organisation and addressed at the strategic and operational level. The outcome of good data security should be a benefit, not a burden.

Data Mapping

It is impossible to start to look at compliance with the various data protection and communication laws without knowing what data you hold, how you treat it and why.

Beyond aiding compliance, there are further benefits of going through a data mapping exercise:

- Identify un-needed data (which is low reward and high risk);
- Spot opportunities to make more of data already held; and
- Make databases leaner, smarter and more efficient.

I have set out below the anatomy of a data mapping process (sometimes called a data audit or data discovery exercise). This is just an example of how our retail and ecommerce clients conduct their map – feel free to deviate as you need, but note that the below is a tried and tested method.

The first step is always to look at the "data journey" within the organisation. Think of this as an x-ray of the organisation. Data will come from one or more sources, and be used in one or more ways (and third parties may use or assist with the use or storage of the data). You might need to interview your staff to identify current practices/habits that you're unaware of. Here's a very basic example for one piece of consumer personal data (e.g. name):

Step 1

Data collection could be direct submission of data by a subject, collation from a number of sources, or gathered by a third party and provided for a fee.

Step 2

The data use might initially be limited – e.g. to process a transaction – with a view to using some or all of the data for future purposes (marketing correspondence).

Step 3

Data is typically stored (often with a third party) with no expiration.

The above example is the most simplistic and, in reality, the data journey for consumer personal data entering your business is likely to be vast and complex with multiple points of storage and processing. To that end, this stage of the mapping exercise should commence as soon as possible.

Fast 5 and Furious 3

Once the map is complete, you need to pick the Fast 5 and Furious 3. It is recommended that you seek legal advice at this time to identify these areas; for example you may find that your existing data can be used post 25 May 2018 as it falls under a PECR exemption.

Fast 5

Process, policies and procedure can produce quick compliance wins where a simple tweak, additional or change can lead to adherence to laws or mitigation of risk. For example, if a person's bank details are being recorded, that process should be mapped out, secure and adhered to.

Looking at your map, pick your "Fast 5" – tweaks, changes or discipline which can reduce obvious risk. If you're found to have a blatant weakness in your system, (e.g. collecting data without seeking explicit and informed consent) criminals will take advantage and regulatory bodies will be more aggressive with penalties. Note that simply having a compliant policy isn't enough; there must be evidence adoption/implementation of it across all levels and training delivered where necessary.

Furious 3

Simultaneous to the above, once your data map is complete you need to pick the “Furious 3” high risk areas where significant improvement is required. These will require considered thought and advice to identify remedy, and an individual in the organisation should be appointed to take ownership of these tasks. If your organisation deals with a lot of personal/sensitive data, this person should be, or may become, your Data Protection Officer.

Review

As the technological landscape constantly evolves, and business changes you will need to keep the data you process and store under review. If you don’t, there’s a danger that your practices and solutions will become outdated – making you an easy target for criminals and high fines.

Please let me know if you have any questions with regard to the above – ordinarily our clients will instruct us to conduct this exercise for them or retain us for support through the mapping exercise to the point that we advise on the methodology and output.

Date: November 2017
Revision: V.1
For more information contact: ip.it@stephens-scown.co.uk or 01392 210700.