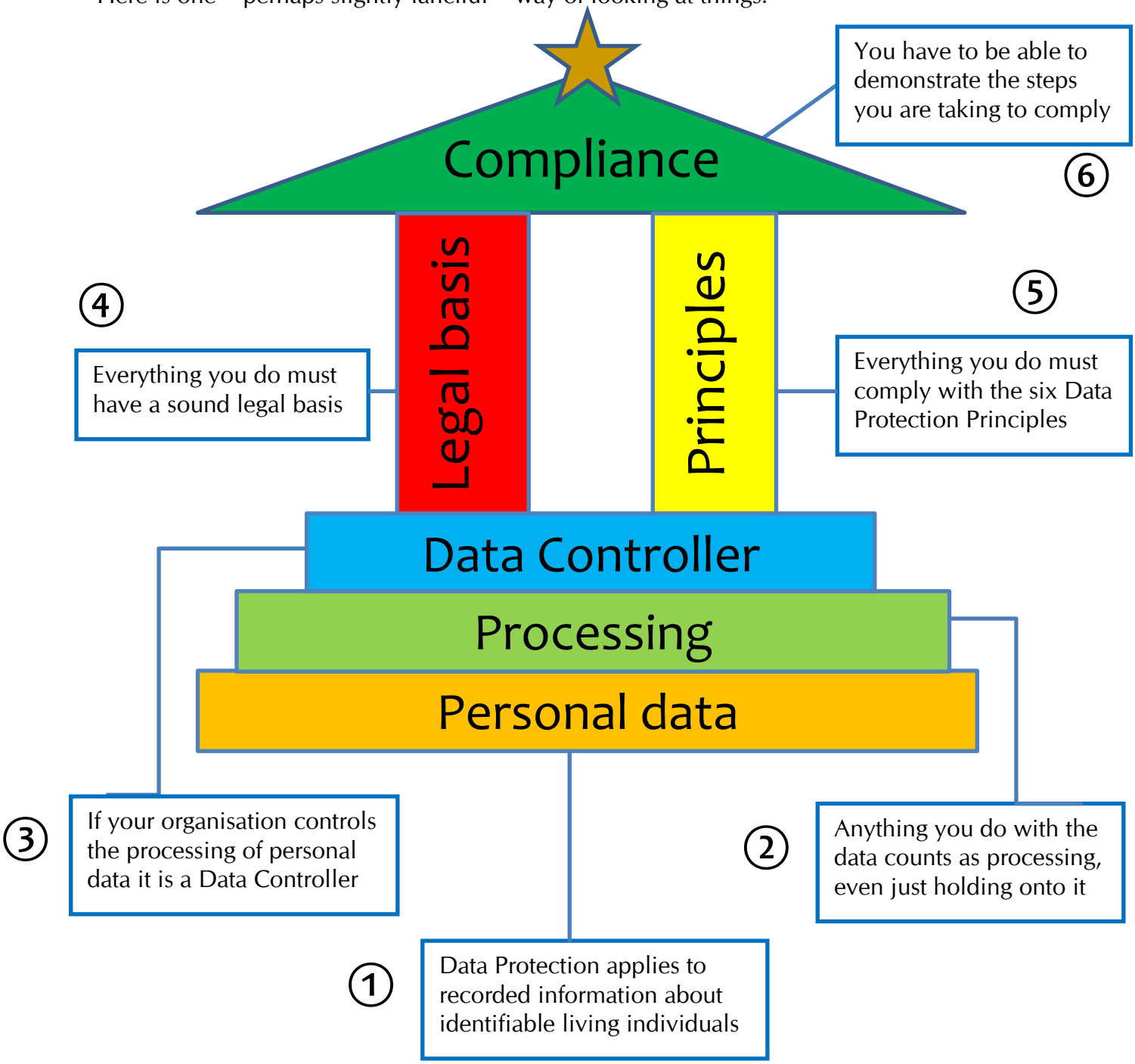
PAUL | TICHER

Data Protection: The elements of GDPR
April 2018

This is my attempt to summarise how GDPR works. This should all be pretty familiar to many people by now, but I thought it might be useful to provide a consolidated exposition that could be used as a starting point with those who have not been following things so closely.

This paper therefore goes right back to basics, and it leaves out some of the complexities. Here is one – perhaps slightly fanciful – way of looking at things:



Personal data

The purpose of Data Protection is to protect people (or "data subjects", as they are technically known). Data about these data subjects is called personal data. This is defined in Article 4 (1) of GDPR as:

> *"any information relating to an identified or identifiable natural person ('data subject');*

GDPR introduces new considerations about how people might be identifiable. Essentially they are 'identifiable' if there is any way of picking that individual out from others and, potentially, treating them differently. You don't have to know their name. Article 4 (1) says:

> *"an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"*

This ties in with the emphasis in GDPR on ensuring that Data Protection covers online activity, among other things.

So, you may have someone participating in an online forum, for example, whom you only know by their username. The information you hold, relating to their posts and other activity, would still be personal data. The same would go for a photograph where someone is clearly distinguishable, even if you don't know their name.

Data Protection only applies to information about living people. That's not stated in GDPR, but it is made explicit in s.3(2) of the UK's Data Protection Bill.

It's also worth noting that Data Protection only applies to *recorded* information, not to things that are just in your head because you have heard or seen them.

These last two points help to explain why Data Protection and Confidentiality are not the same thing (even though they do often overlap). Confidentiality might apply to information about people after they have died; it might apply to things you have witnessed but not recorded; and it might apply to information about organisations.

Data Protection, on the other hand, would apply to personal data that is in the public domain, and therefore not confidential.

It's worth thinking about where your organisation holds personal data. Some places are obvious: your database or CRM system, the user data on your website, your paper files. Others may not immediately come to mind: in many organisations the largest amount of personal data is probably to be found in emails.

Every time you write or receive an email about one or more people (even without them being named, in most cases) you are creating or acquiring personal data about them.

Processing

Data Protection applies whenever personal data is 'processed'. This doesn't just mean getting a computer to do something with it. Section 4 (2) of GDPR defines it as:

> *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"*

This is pretty comprehensive. It would include, for example, just reading personal

data onscreen or in a paper file, even if you don't do anything else with it. It would include storing archives of personal data (and it would also include shredding it instead).

(Data) Controller

Any organisation is a Controller under GDPR if it "determines the purposes and means of the processing of personal data".

(Under the previous legislation the term 'Data Controller' was used, which is less ambiguous and will sometimes be used in this paper to avoid any confusion.)

Individuals can also be Controllers in respect of any business activities on their own account, but it is understood that the current exemption for "domestic purposes" will be retained.

GDPR recognises that collaborative working happens, and that two or more organisations might be joint Controllers of a set of data or a set of processing activities. In this case, Article 26 says that:

> *"[Joint Controllers] shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information …"*

In other words, the organisations involved have to have a clear idea of who is going to do what, in order to ensure full GDPR compliance, and to understand what will happen if they don't do their bit properly.

If you pay another organisation to carry out processing for you, and if they have to act on your instructions, they are a Processor (or 'Data Processor' in old money). This could cover a vast range of suppliers, including a payroll company, a web developer, a freelance photographer, an archive storage repository …

GDPR sets out a list of things that must be covered in your contract with a Processor. If they follow your instructions, you are responsible for any breach they cause. If they don't, however, they can be directly liable. This makes it very important to check your contract, so that the Processor's responsibilities are clearly set out.

Legal basis

Everything you do has to have a legal basis, chosen from among the six set out in GDPR. These are (briefly):

- With consent of the Data Subject
- For a contract involving the Data Subject
- To meet a legal obligation
- To protect any person's 'vital interests'
- Government & judicial functions
- In your 'legitimate interests' provided the Data Subject's interests are respected

You do not have to use the same basis all the time, even for related bits of data. With employees, for example, your key employment records would be on the basis of contract; your disclosure of payments to HMRC would be a legal obligation; some information in your personnel records might be held on the basis of legitimate interests, because it was worth having, but not essential for the contract; other information – for genuinely optional matters – might only be held with consent.

The key thing is to be clear in every case what your legal basis is. (See also the discussion on transparency, below.)

It is usually not difficult to identify cases where one of the four bases in the middle of the list apply. There has, however, been much debate over how to decide between consent and legitimate interests, especially in the case of direct marketing.

The Information Commissioner has issued useful guidance on legitimate interests, saying:

"Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate. It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing."

It is generally agreed that there has to be a three-stage test in order to establish whether legitimate interests is a valid legal basis:

- What is our legitimate interest?
- Why is the processing necessary?
- Does our interest outweigh the data subject's interests?

This is described in much more detail in the ICO Guidance – which confirms that legitimate interests may in some cases be used as the basis for direct marketing.

Direct marketing

Direct marketing probably merits a briefing of its own, since it has raised so many concerns, but it is worth a short overview here.

The Information Commissioner's Direct Marketing Guidance considers that direct marketing includes:

"… any advertising or marketing material, not just commercial marketing. All promotional material falls within this definition, including material promoting the aims of not-for-profit organisations.

It will also cover any messages which include some marketing elements, even if that is not their main purpose."

This is a very broad definition, and would include, for example, an e-newsletter that is mainly information about your activities, with a small amount of encouragement to support or participate in them.

GDPR says that direct marketing may be a legitimate interest. (Note the "may be". It's not automatic.) You almost certainly can't base all your marketing on legitimate interest, because the ePrivacy Regulation (currently the Privacy & Electronic Communications Regulations, but in the process of being revised) says that you need consent in certain circumstances for marketing by phone, email or text message. Many charities have decided that it is easier to carry out all or most of their electronic direct marketing on the basis of consent.

In the case of direct marketing by mail, however, the question is what you have to do if you want your legal basis to be legitimate interest. Basically there are two requirements: you have to tell people in advance that you are going to use their data for direct marketing — which in the case of new donors would be at the point where you first capture their details; and you have to tell them that they have the right to opt out, and give them an easy way of doing so. In other words you need, as a minimum, a clear statement and an opt out box.

There are obviously some advantages in being able to mail people who haven't given you consent, which is why many charities are taking this route. The down-side is that it makes your data capture forms and data management more complicated, because you would be working on an opt in basis for electronic contact and an opt out basis for mail.

So you have to make a decision and then make sure that all your processes, systems and paperwork support that decision accurately.

Principles

Under the Data Protection Act there are eight Data Protection Principles. GDPR introduces very little change.

There is a small difference in the wording of the third Principle, while the sixth (respect for Data Subject rights) and eighth (limitations on transfers abroad) from the DPA are omitted (but covered in detail elsewhere in GDPR).

The six GDPR Principles are therefore that personal data shall be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes …;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to [erase or rectify] personal data that are inaccurate … without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary;
- 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.

No one can (or certainly should) argue against holding good quality data and looking after it properly. However, the biggest change under GDPR is the much greater emphasis on genuine transparency.

Transparency

The list of information that must now be available to Data Subjects is lengthy. Clearly it cannot be provided in full every time data is obtained, so a 'layered' approach is required: a full privacy notice that is available on request or to download, and probably provided to people as part of a welcome pack, or similar; and shorter notices giving key information and options at each point of data capture.

The Principles

- **Lawfulness, fairness and transparency**
- **Purpose limitation**
- **Data minimisation**
- **Accuracy**
- **Storage limitation**
- **Integrity and confidentiality**

The full transparency list includes:

- the identity and the contact details of the controller and its Data Protection Officer (if there is one)
- the purposes as well as the legal basis of the processing
- where relevant the legitimate interests
- any recipient(s)
- any overseas transfers
- the storage period or criteria for deletion
- right of access to data and rectification or erasure
- right to withdraw consent at any time (if that is the legal basis being used)
- right to complain to the ICO
- whether the provision of personal data is [contractually] required [or] the data subject is obliged to provide the data and … possible consequences of failure to provide [it]
- the existence of automated decision-making, including profiling, and the envisaged consequences

Where the data is not obtained from the individual they also have to be told:

- the categories of personal data involved
- the source of the personal data

It is in any case a worthwhile exercise to compile the full privacy statement, in order to demonstrate that your organisation has a thought-through approach to its processing and to its relationship with Data Subjects.

It is also important to compose clear and succinct statements for each situation in which data is captured, so that Data Subjects are able to make an informed

judgement about whether or not to provide their data.

It makes sense for your communications team to be involved in drafting your privacy notices, but they should not be left to determine the content. GDPR is very particular about what gets included, even if it means telling people things you might prefer not to disclose.

Data quality and retention

Although your existing processes for ensuring data quality are unlikely to need much change, it is worth considering – especially in view of the transparency requirements – producing a full data retention schedule, setting out how long different classes of data are held, and why this retention period has been set.

An area that can be over-looked in terms of retention is email. Personal data in emails (either in the content or in any addresses that identify the individual) is typically not stored in a structured way that permits its easy identification for deletion. However, the obligation to hold it no longer than necessary should be respected.

Security

Data security must clearly be a major concern. However, if your existing security is fit for purpose there is probably little that will need changing.

It may be worth taking the opportunity to review your security, however. Key areas you may want to address include:

- Data 'in transit'
  - access/encryption on phones, tablets USB devices and laptops
  - extreme care when e-mailing (encryption?)
  - care of confidential documents
- Network security – anti-virus, firewall, log-ons, etc
- Website security
- 'Bring Your Own Device policy' and working from home policy
- Policy on use of cloud applications
- Access to building, clear desks, locked filing cabinets
- Secure destruction – shredding, etc.
- Staff reliability: checks, supervision, monitoring
- External contractors ('Data Processors')

It is worth remembering that the maximum penalty for a Data Protection breach rises from £500,000 to £17,000,000 – although the Information Commissioner has said that the actual penalties levied will, in most cases, be near the current levels.

Compliance

Some of the remaining matters that are involved in full compliance include:

- Breach notification: there is now a mandatory requirement to report serious breaches within 72 hours.
- An extended list of Data Subject rights, including rights to prevent processing or have their data erased in certain cases.
- A requirement to keep records that can demonstrate the steps the organisation has taken to comply with GDPR.
- Data Protection 'by design and by default', so that it is taken fully into account whenever a new activity or process is set up.
- Greater protection where data is held on or acquired from children.

I'm an independent specialist, with over 30 years' experience of Data Protection in the voluntary sector.

However, I'm not a lawyer. This paper may not be a complete or accurate statement of the law, and it is not intended to be legal advice.

If you have any questions on this paper, please do contact me: on 0116 273 8191 or paul@paulticher.com.