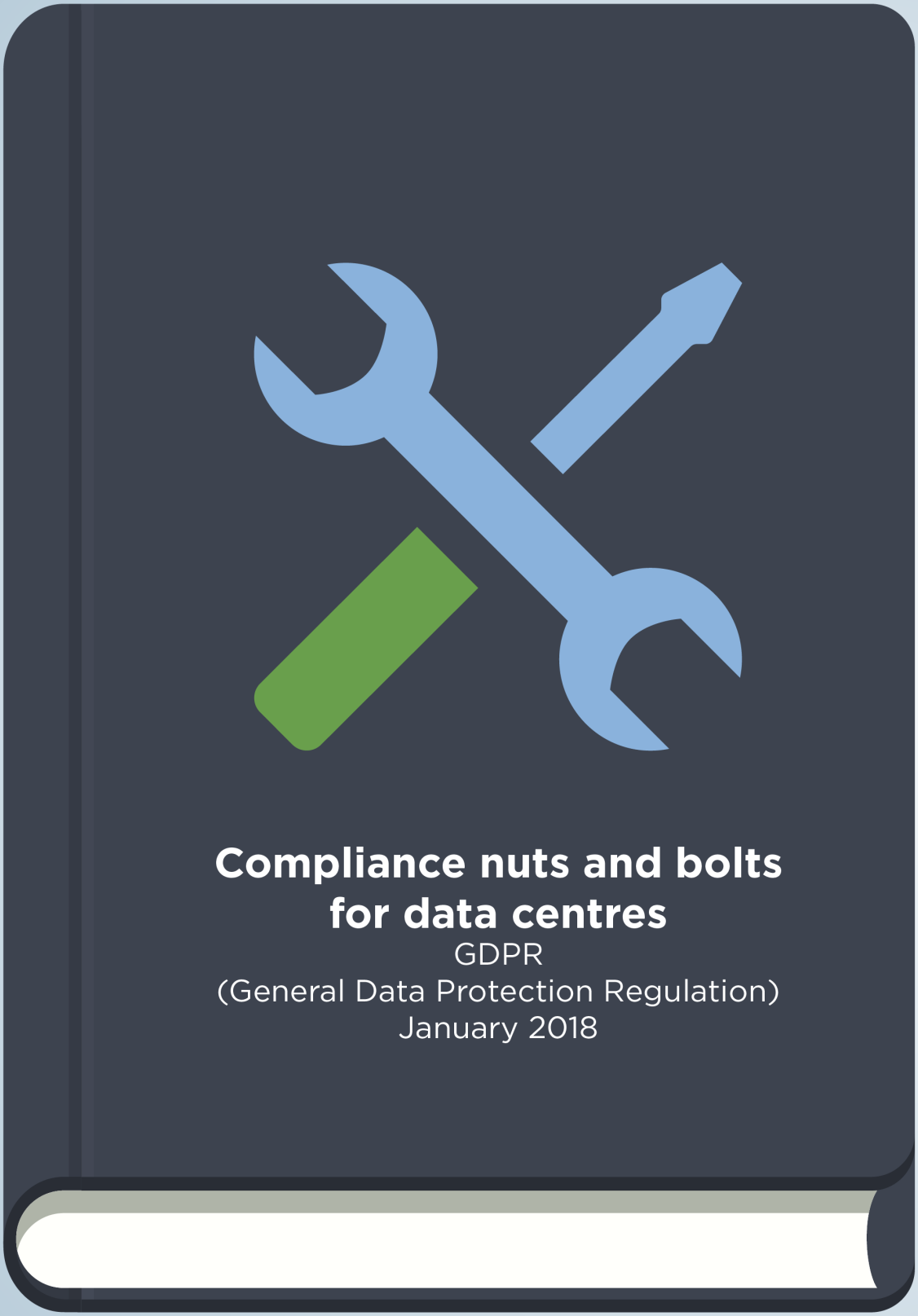
techUK



# Compliance nuts and bolts for data centres

GDPR
(General Data Protection Regulation)
January 2018

**GDPR is causing confusion among data centre operators who are struggling to understand whether and how it applies to them.**

The answers are "almost certainly" and "it depends", respectively. The following notes are designed to help operators understand their general compliance obligations based on their activity and business model. They summarise the main issues and why they matter.

Two decision trees help operators establish firstly whether they are data controllers and secondly whether they are data processors. Some quick action tips and links to useful third-party reference materials are also included.



NB: These notes are only intended as a rough rule of thumb and are not comprehensive, nor should they be regarded as a substitute for professional or legal advice. They are complementary to, and should be read in the context of, other advisory and reference sources such as those listed over the following pages.

## 1. Why is GDPR so Confusing for Data Centre Operators?

GDPR – the General Data Protection Regulation, takes effect on 25th May 2018. It harmonises data protection laws across the EU and updates previous legislation (in the UK's case the Data Protection Act 1998). The new Regulation accommodates our move to digital data and online business models but also applies to non-digital personal data. Organisations that comply with the 1998 Data Protection Act (all should!) will be on the way to GDPR compliance, as will those with ISO27001. However, this is not a time to rest on laurels because some changes introduced by the new Regulation are particularly pertinent for data centre operators and operators of IT services within data centres.

### What has changed?

1. Liability has extended to include data processors. Now data controllers and data processors potentially have joint and several liability. The definition of a data processor has not changed.
2. The definition of personal data has been broadened, and there is now a right to be forgotten amongst other enhanced rights for data subjects such as right of action.
3. You don't just have to comply with statutory obligations, you also have to document your compliance and keep appropriate records as part of the accountability principle.
4. Data breach notification rules are now compulsory and the maximum fine for breaches increases from £500,000 to €20M or four per cent of global turnover, whichever is greater, for some offences.

### Why does this matter for everyone?

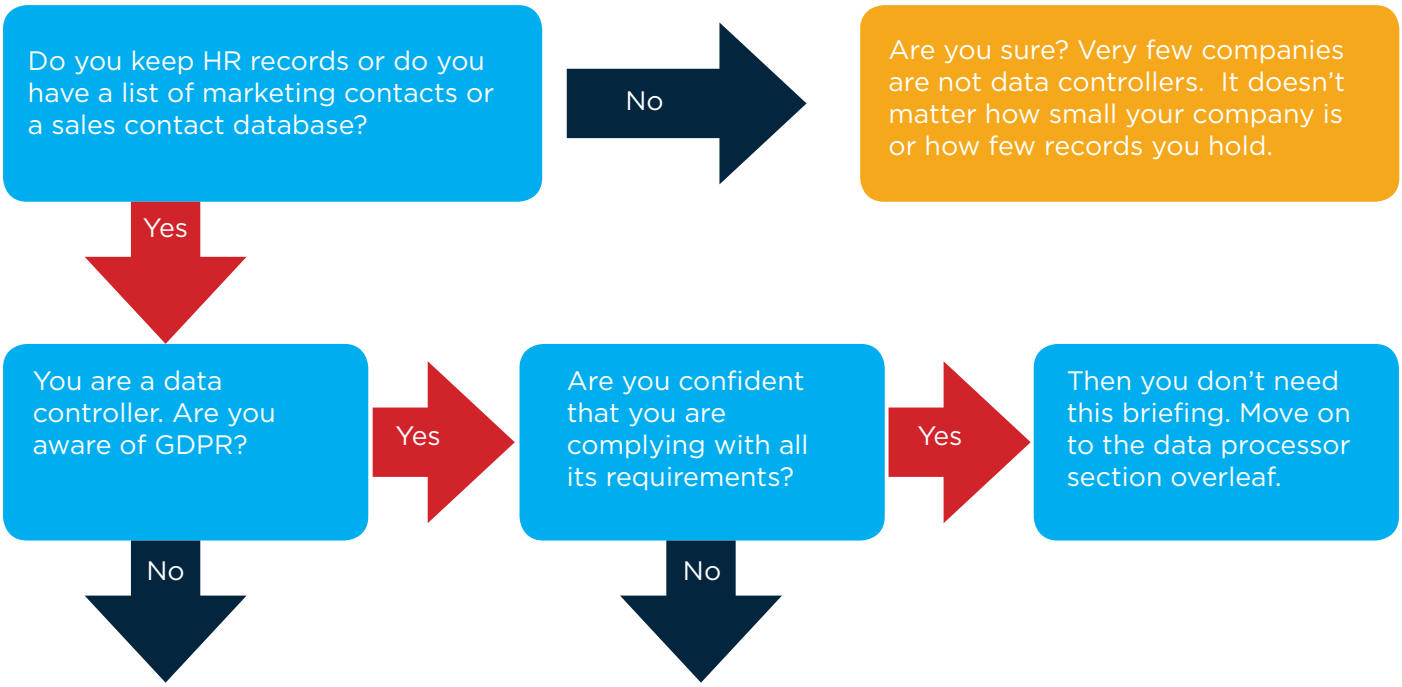
It matters because GDPR applies to any organisation of any size in any sector that processes any kind of personal data, including any personal information on any EU residents, due to the extra-territorial nature of GDPR.

### What is the issue for data centre operators?

Data centre operators are controllers of their own data (e.g. HR and payroll, sales and marketing lists, CCTV and access logs) but, depending on their activities, may also be processors of data that is controlled by third parties, data that they have no access to or control over. Establishing whether an operator is – or is not - a data processor is not always straightforward. So data centre operators potentially have dual liability under the legislation: firstly as data controllers of personal information that they hold, store and process for their own purposes, and secondly as data processors of data held within their facilities by third party data controllers – their customers. Operators may have different responsibilities depending on status: controllers must comply with GDPR; processors now have direct responsibility, including an obligation to help the controller to comply. The following pages should help operators establish which duties might apply to them and whether they are indeed likely to be data processors, as well as controllers.

## 2. Are You a Data Controller?

**A data controller is: "a natural or legal person, public authority, agency or other body which, either alone or jointly with others, determines the purposes and means of processing of personal data".**[1]




Have you been living on Mars for the last few years? GDPR is the most fundamental change to our data protection laws in over 20 years and will impact digital and data intensive businesses in particular.
Fundamentally, if you hold personal data of European citizens, GPDR requires you to keep that information secure and to make sure that individuals' rights are respected.
You need to know what data your hold, where it comes from, where precisely it is.
Read the guidance from the Information Commissioner's Office, the ICO. See links below.

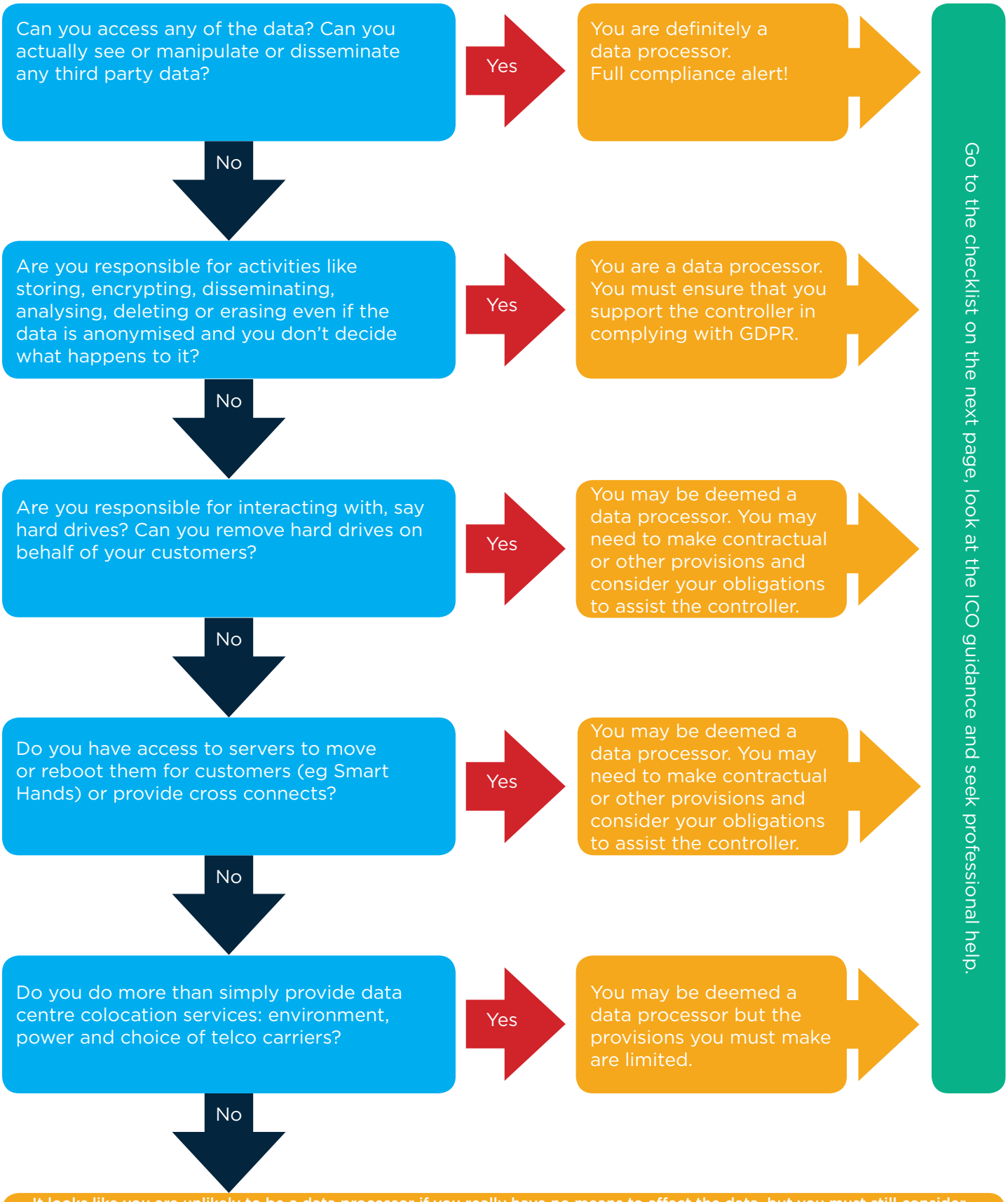
**Controller? Here's what you need to do:**

- Read the useful briefings from the ICO (see links below).
- Identify and alert relevant individuals within your organisation to changes to data law.
- Assess whether you need to designate a data protection officer.
- If necessary, conduct an information audit.
- Ensure that you document what personal data you hold, where it is, where it came from and who else has access to it.
- Ensure your suppliers (processors) are GDPR compliant, aware of their obligations and can demonstrate this, especially if overseas. This has to be formalised in contracts.
- Ensure you have procedures for handling information requests, subject requests and recording of consent.
- Ensure you can comply with new breach notification requirements.
- Review your risk register, privacy notices, policies and procedures to ensure they meet GDPR requirements.
- Prioritise security arrangements according to the new risk based approach (e.g. security from theft, robust anonymity protection).
- Conduct a Privacy Impact Assessment if necessary.
- Train staff and communicate with customers to advise them of changes in law.
- Align your GDPR compliance with certifications and other standards you comply with.

1 'GDPR Article 4 (7)'

## 3. Are You a Data Processor?

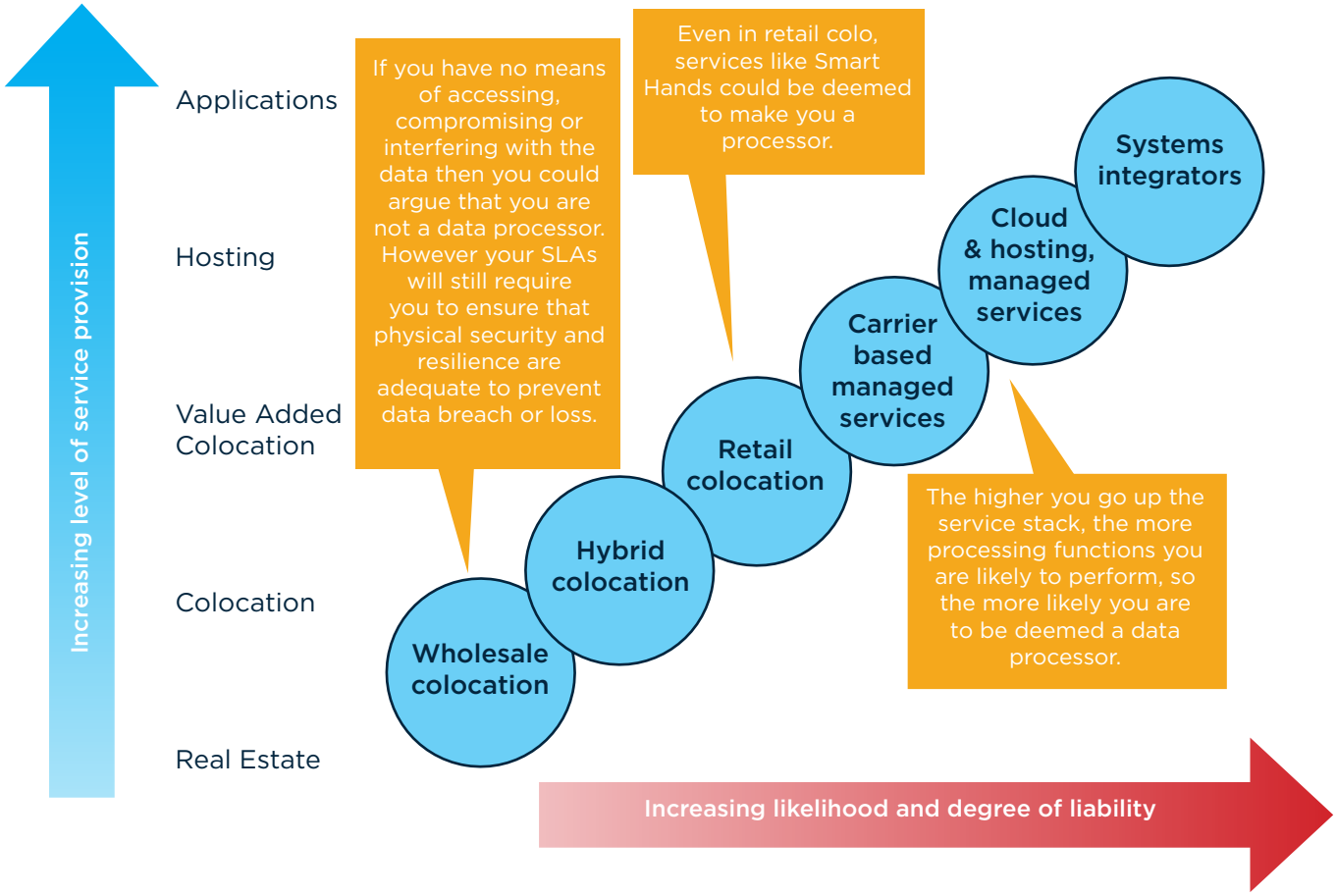
**A data processor is: "A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."**[2] But really the question you need to ask is: "Can you in any way affect the data, and if so, to what extent?" The extent matters because the precautions you take will be proportional.




**It looks like you are unlikely to be a data processor if you really have no means to affect the data, but you must still consider physical security and contractual obligations. Moreover, if you start adding services in future then you have to re-examine your status and liabilities.**

2 'GDPR Article 4(8)'

**Where in the service stack are you deemed to be a data processor?**
This image is another way of assessing the kinds of operators likely to be considered data processors. In reality, the level at which one becomes a data processor is likely to be defined by case law.




**So, you ARE a Processor. Here's what you need to do:**

- Read the useful briefing from CRS on GDPR for IT Services (see links below).
- Identify and alert relevant individuals within your organisations to changes to data law and the new obligations for processors: increased liability, more detailed contractual requirements, provision of guarantees to controller, requirement to support controller compliance, etc.
- Ensure you understand and can meet the technical and organisational requirements.
- Review contract changes required by controllers to ensure that liability is balanced and is not being shifted down the supply chain.
- Implement processes for reporting data breaches in line with GDPR.
- Audit compliance processes to ensure they are GDPR ready.
- Communicate with the data controller: transparency is critical to ensure that you have the same understanding of risks, responsibilities and respective liability.
- Revisit contracts and review if necessary.
- Consider adopting;
  - Insurance
  - Codes of conduct/certifications
- Ensure you have permission from the controller for the use of sub-processors.
- Ensure suppliers, especially sub-processors, are aware of their obligations, can demonstrate this and contracts reflect this.
- Prioritise security arrangements according to the new risk based approach (e.g. security from theft, robust anonymity protection).
- Document all steps taken, including training.

## 4. Links, References and Definitions

### Links and References

ICO: Overview of the GDPR

ICO: Preparing for the GDPR: 12 steps to take now

ICO: What to expect and when

ICO: Getting Ready for the GDPR: SME Checklist

Charles Russell Speechlys: GDPR for IT Services: Keeping compliance at the heart of the controller/processor relationship

Charles Russell Speechlys: Bringing Clarity to the Cloud

techUK, UK Finance and Dentons: No interruptions: Options for the future UK-EU data sharing relationship

techUK: How will new EU data rules impact my tech business?

techUK: Data Protection Bill Begins its Parliamentary Journey


### Acknowledgements

Mark Bailey, Charles Russell Speechlys LLP
Mitul Patel, CBRE


### Further Information


**Data Centres**
Emma Fryer
Associate Director, techUK
T 01609 772 137
M 07595 410 653
E emma.fryer@techuk.org

**GDPR**
Jeremy Lilley
Policy Manager, techUK
T 020 7331 2023
M 07545 204 098
E jeremy.lilley@techuk.org


**MORE DEFINITIONS...**

**Personal data:** Any information relating to an identified or identifiable natural person ('data subject'); 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. It should be noted that this definition has been expanded compared to the DPA 1998.[3]

**Data processing:** 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.[4]

3 'GDPR Article 4(1)'
4 'GDPR Article 4(2)'

techUK

**techUK represents the companies and technologies that are defining today the world that we will live in tomorrow.**

The tech industry is creating jobs and growth across the UK. 950 companies are members of techUK.

Collectively they employ more than 700,000 people. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium sized businesses.

**www.techuk.org | @techUK | #techUK**