I’m very much looking forward to Datacloud in Monaco next month where I will be chairing a session on GDPR. It’s a rollercoaster of a programme and we have a very short time slot so we will need to get stuck straight into the content without the luxury of much scene setting. So I thought it would be worth providing a reminder of the main issues GDPR presents to data centre operators and cloud service providers and a taster of the topics that we will explore in the session. It also gives me the opportunity to share a few of my own thoughts and concerns about GDPR.

The first thing I should say is that I am not an expert on GDPR. Although it is an issue that techUK has been very actively engaged in for the last four years it is not specific to data centres and because of its wide remit, the policy dialogue is led by a specialist team within techUK. Fortunately I get to ride shotgun on the process because the implications for data centre operators and cloud services providers are very significant.

So what is the GDPR?
The GDPR is a wide ranging EU regulation that aims to strengthen consumer protection and enhance trust and confidence in how personal data is used and managed. It will replace existing legislation that has been in place since the mid-1990s (Directive 95/46/EC). It is intended to be one of the key regulatory cornerstones for Europe’s ambition to be a leading global digital economy. The regulation covers the way personal data is gathered, stored, shared, processed and used.

GDPR does not just affect technology companies: it will impact all businesses handling personal data, even small amounts – a vast range of organisations across multiple sectors. Geographically, GDPR will apply to businesses across the global economy - not just those actually located in the EU but also those based elsewhere if they process the personal data of European residents and offer them goods and services. GDPR will come into force on 25th May 2018.

GDPR is one of the most amended pieces of legislation in history and the negotiations have lasted over four years and have generated a lot of controversy. The main issues that GDPR presents for businesses are summarised in Box 1.

<table>
<thead>
<tr>
<th>Box 1: Main issues identified in GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Unambiguous consent still required (Articles 4 &amp; 6)</td>
</tr>
<tr>
<td>2. New liabilities and obligations for data processors (Article 77)</td>
</tr>
<tr>
<td>3. Restrictions on the use of 'legitimate interest' as a legal basis to process data (Article 6)</td>
</tr>
<tr>
<td>4. New restrictions on the use of profiling to support products and services (Article 20)</td>
</tr>
<tr>
<td>5. Innovation and further processing (Article 6)</td>
</tr>
<tr>
<td>6. Notification requirements for data breaches and increased penalties (Article 31 &amp; 32)</td>
</tr>
<tr>
<td>7. Potential for fragmentation regarding the way children's data is handled(Article 8)</td>
</tr>
<tr>
<td>8. A requirement for businesses to appoint a Data Protection officer (Article 35)</td>
</tr>
<tr>
<td>9. International Data Transfer requirements (Article 43a)</td>
</tr>
</tbody>
</table>

There are exemptions for SMEs and for public sector bodies.
What are the issues for data centre operators?

From my perspective, working with data centre operators and cloud service providers there are three overriding areas of concern. These are: 1) the definition of personal data, 2) joint and several liability and 3) penalties. They are closely connected and between them they change the liability landscape for operators. This is how:

**Definition of personal data:** the new regulation has expanded the definitions of personal data as any data that can "directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;" This broadening of the definition means that a much wider range of information can now be deemed to be personal data than previously.

**Joint and several liability:** Data controllers¹ and processors² will have joint liability for any breach of the Regulation. This extends responsibility beyond the companies that collect and use personal data (data controllers) to organisations in the supply chain that simply provide the equipment on which that data is processed or stored. Cloud-providers, data centres and processors will now be liable for data held on their services even if they are not data controllers. Given that these data processors will have little visibility over whether the data collected by data controllers is compliant with the new Regulation, managing the legal implications of this requirement within contracts between controllers and processors will be difficult and potentially costly. This means that customers, particularly SMEs will be faced by higher costs. Consumers will also be faced by a complex legal environment where there is less clarity about who is liable in the case of data breaches.

**Penalties:** the requirements for notifying consumers of data breaches have changed. New mandatory breach notifications will have to be made within 72 hours of companies discovering a data breach. The Regulation will also introduce much more punitive fines for companies that are found to be non-compliant with the Regulation. Business could be fined up to four per cent of global revenue, or 20 million euros, depending upon the nature of the compliance failure.

What do I want to know about GDPR?

When I think about all these changes, three questions spring to mind.

Firstly, where in the data centre stack will this strike? If you are a pure wholesale colocation provider you can probably argue that you are not a data processor, but the addition of even quite basic services could have an impact on legal status. The fact that personal data is running through your networks may make you a data processor under the new rules. We will need clarification from the ICO (Information Commissioner’s Office), access to good legal advice and, unfortunately for

¹ See Article 4 (7): ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

² See article 4 (8) ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
some, a bit of case-law under our belts before we really know how the land lies and even then the variety and complexity of business models and service mixes means that rules of thumb may be very elusive.

**Next question, how will they decide who is to blame?** Let’s take a fictional scenario.... Mr Silly, a data controller who should know better, is using his laptop to check customer salary records while he is having a coffee in Starbucks on an open wifi system. These salary records are actually held a hundred miles away in a secure data centre surrounded by barbed wire, with bomb proof walls and biometric security, policed and managed by Mr Strong. The computers on which the data is held belong to a cloud services provider, Mr Worry, who provides the platform on which the data is hosted. Mr Nosey, who is sitting next to Mr Silly in Starbucks having a latte and a pecan Danish and enjoying a chat with his friend, Mr Mischief, sees what Mr Silly is doing and notices that there are some very interesting salary packages there. Mr Mischief hacks in and forwards a whole load of sensitive information to Mr Chatterbox at the Daily Mail. There is a big scandal and heads must roll. Who is to blame under the new GDPR? The data controller; Mr Silly? The data centre operator: Mr Strong? The cloud services provider; Mr Worry? Starbucks? The sandwich delivery boy? Some bloke who happens to be passing in the street? All of the m? All of the m? What about Mr Nosey, Mr Mischief and Mr Chatterbox? Shouldn’t they be on the list? And who decides who is to blame?

**And how much does everyone get fined?** The fines can be up to four per cent of global turnover or 20 million euros, whichever is higher, so it would be useful to know whose turnover. If the data controller, say, is a huge retail giant with a multi billion pound operation, how is the fine for a major data breach apportioned down the supply chain? How would this affect smaller operators who provide hosting or colocation services?

This all leaves me with one critical question. How should European data centre operators and cloud service providers prepare for 25th May 2018?

Our panellists will shed light on these and other questions at our session at Datacloud, and I for one am very much looking forward to it. In the meantime, if you need more information on the implications of GDPR on the technology sector, or on the position that techUK has taken on behalf of the sector, then have a look at some of the links below.

techUK has published a number of consultation responses and policy positions on GDPR, and is also running an event on 25th May “Will GDPR Change the World?” with Rob Luke, Deputy Information Commissioner, and a training course on 12th July “An introduction to the UK Data Protection Act and UK GDPR”.

For more information about our cloud computing and data protection programmes, please contact Sue.daley@techuk.org or jeremy.lilley@techuk.org. For courses, please contact mariana.obetzanova@techuk.org

Emma Fryer will be chairing “The Brave New World of GDPR” at DataCloud 2017, on 7th June at 4pm in the Innovation and Investment theatre. She will be joined by:

- Gayle McFarlane, Partner, Eversheds Sutherland
- Garry Connolly, President, Host in Ireland
- Tom Kettels, Chief Business Development Officer, LuxConnect
- Claudio Caimi, Program Manager - Security Team, Discovery Project partner, HPE

If you haven’t yet registered for Datacloud and are planning to go, you can get a 15% discount if you use the techUK discount code: BNC5A7 when booking. See: http://www.datacloudcongress.com/

Emma Fryer, Associate Director, techUK
May 2017
Emma.fryer@techuk.org