to national legislation with potentially additional objectives without the CJEU expressly stating so.

As a matter of fact, national data retention laws must comply with EU law. If the EU legislation setting the rules for domestic data retention laws is invalidated for breach of fundamental rights guaranteed under EU law, the national laws implementing (and therefore, at least in principle, mirroring those rules) would be highly likely to breach those same rights and laws. Therefore, the CJEU ruling must have at least some (indirect) effect on national data retention legislation and provide some measure when it comes to assessing the compatibility of national data retention laws with EU law.

Given the Court of Appeal has asked for the CJEU proceedings to be expedited, some much-needed clarifications might be forthcoming soon. Finally, the Presidency of the European Union on 24 November 2015 invited the EU Ministers to consider whether the EU Commission should be invited to present a new legislative initiative on data retention. Well, that data retention debate seems far from over…

• This article was first published on www.bakerinform.com

‘Main establishment’ under the GDPR and the NIS Directive

Charlotte Mullarkey analyses how the job of determining main establishment differs between these two new pieces of legislation.

One of the key changes proposed by the European Commission four years ago in its revised data protection framework was its vision of a “One Stop Shop”. This is the idea that a single authority in one Member State has responsibility for a company or group of companies’ data processing activities and compliance across the EU. Over years of discussion, the regime has evolved somewhat into what now appears in the agreed text of the resulting General Data Protection Regulation (GDPR), but the principle still remains largely intact. Key to the regime is identification of a lead data protection authority, which hinges on where the ‘main establishment’ of a company/group is located.

As companies grapple with this, the Network and Information Security Directive (NIS Directive), the text of which has also recently been agreed, introduces a similar concept for regulation of the networks and information systems of digital services providers. This means identifying a lead authority for those digital services providers which operate across the EU.

As the criteria for identifying a ‘main establishment’ differs across the two pieces of legislation, and the relevant authorities are likely to be separate in each Member State, this raises the questions: how will this work in practice and should we expect more ‘One Stop Shop’ regimes to spring up in other pieces of legislation being reviewed at an EU level using different criteria?

ONE STOP SHOP UNDER THE GDPR

The One Stop Shop idea sees a European Union in which a company or group of companies that operates across more than one Member State would have one regulatory point of contact. As this concept evolved through the intense lobbying and discussions around the proposed GDPR it became more complex but arguably more workable in practice. The agreed regime means that a company will have one lead supervisory authority for data protection compliance across the EU. This lead supervisory authority would then work with other ‘concerned’ supervisory authorities in other Member States and there is a detailed mechanism for their cooperation, with disagreements between authorities going through a consistency mechanism. There is also a detailed regime for dealing with local cases.
It has been difficult enough for people to get their heads around this “main establishment” idea. Critics believe forum shopping could distort the system, something the Commission vigorously denies, pointing to the detailed consistency mechanism for cases of dispute. There are also concerns about resources in certain (perhaps all) supervisory authorities and a bottleneck if too many cases are referred up to the EDPB (the European Data Protection Board) through the consistency mechanism. These organisations have not traditionally had extensive resources.

**JURISDICTION OF REGULATORY AUTHORITIES UNDER THE NIS**

The GDPR does at least have the advantage of being a Regulation. As such, it does not need to be implemented locally in Member States. It may come as a surprise to some therefore that a similar idea has been introduced in the final text of the NIS Directive in relation to compliance by digital service providers (i.e. providers of online marketplaces, online search engines and cloud computing services). Here, what the GDPR took many pages to describe is introduced in just a couple of paragraphs.

Under the NIS Directive, the supervisory authority of a digital service provider’s ‘main establishment’ will have jurisdiction for that company or group of companies across the EU. This sounds the same as the position under the GDPR but the devil, as always, is in the detail.

Where a company is not established in the EU there appears to be plenty of scope for forum shopping as it can effectively appoint its representative in any Member State where it provides services.

For those companies that do have an establishment in the EU, there is perhaps less room for manoeuvre. However, the Recitals to the NIS Directive are less black and white about the test for the “main establishment” than the relevant article itself. They state that “in principle” it is the head office and go on to say that establishment implies the effective and real exercise of activity through stable arrangements. This is similar to the objective test in the GDPR. However, it is less flexible as it does not relate to where the decisions about security are taken.

Additionally, note that “competent authority” in this context means the one designated (as required by the Directive) for network and information systems. The role may be designated to an existing authority (or authorities), but there is no requirement for this to be the same authority that deals with data protection, for example. Interestingly, supervision by the competent authority is to be light touch, only taking action when provided with evidence of non-compliance – there is no general obligation to supervise.

**WHERE DOES THIS LEAVE US?**

For the same company, it is very possible that the ‘main establishment’ for the purposes of the NIS Directive will be different from that for the GDPR. This may cause confusion and lead to over-reporting or under-reporting, and it is unclear how it would work in practice where a cyber-incident also involves the loss of personal data. The Recitals to the NIS Directive do recognise that the relevant competent authorities and data protection authorities will need to cooperate and exchange information. It will be a burden, however, not only to deal with two lead authorities, but also in different EU Member States. This will be particularly relevant for data breach notification/security incident reporting.

With the EU’s Digital Single Market Strategy in full throttle, it remains to be seen if we will see more definitions of “main establishment” in this context in other regulated areas. The UK government only recently warned against using different definitions for the same phrases/ideas in the review of legislation. As the definition in the GDPR is closely tied to the location where decisions are made about processing data, this will clearly not work as a universal definition. Perhaps this will be clarified as the texts go through technical checking in the coming months, or perhaps the vision of a One Stop Shop regime is already being diluted. Many will hope that other EU legislation does not compound the complexity that is being created and dissolve the vision completely.

---

**HOW DO YOU IDENTIFY YOUR COMPETENT AUTHORITY UNDER THE NIS DIRECTIVE?**

If a digital service provider has its main establishment (or a representative) in one Member State, but its networks and information systems are located in one or more other Member States:

- It shall be deemed to be under the jurisdiction of the Member State where it has its main establishment (i.e its head office in the EU) – this does not depend on where the network and information systems are physically located.

- If not established in the EU but providing digital services to the EU it shall designate a representative in one of the Member States where services are offered and that shall be its main establishment.

- The competent authority of the Member State of the main establishment (or of the representative) and the competent authorities of the other Member States shall cooperate and assist each other as necessary.

---

**AUTHOR**

Charlotte Mullarkey is a Senior Professional Support Lawyer at Allen & Overy LLP. Email: Charlotte.Mullarkey@AllenOvery.com

**REFERENCE**

Join the Privacy Laws & Business community


PL&B’s United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others’ experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation’s compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all PL&B publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
You will be sent the PDF version of the new issue on the day of publication. You will also be able to access the issue via the website.

You may choose to receive one printed copy of each Report.

3. E-Mail Updates
E-mail updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

4. Back Issues
Access all the PL&B UK Report back issues since the year 2000.

5. Events Documentation
Access UK events documentation such as Roundtables with the UK Information Commissioner and PL&B Annual International Conferences, in July, Cambridge.

6. Helpline Enquiry Service
Contact the PL&B team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

To Subscribe: [www.privacylaws.com/subscribe](http://www.privacylaws.com/subscribe)

I particularly like the short and concise nature of the Privacy Laws & Business Reports. I never leave home without a copy, and value the printed copies, as I like to read them whilst on my daily train journey into work. Steve Wright, Chief Privacy Officer, Unilever

Subscription Fees

Single User Access
UK Edition £400 + VAT*
International Edition £500 + VAT*
UK & International Combined Edition £800 + VAT*

* VAT only applies to UK based subscribers

Multi User Access
Discounts for 2-4 or 5-25 users – see website for details.

Subscription Discounts
Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.

Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

International Postage (outside UK):
Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30
Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee
If you are dissatisfied with the Report in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the International Report.

[www.privacylaws.com/int](http://www.privacylaws.com/int)