Changes are expected to the EU One-Stop-Shop mechanism

Patrick van Eecke, **Loriane Sangaré-Vayssac** and **Enrique Capdevila** of Cooley analyse the updated guidelines for identifying the Lead Supervisory Authority and the draft GDPR Procedural Regulation.

Following the adoption of the final version of the European Data Protection Board (EDPB) Guidelines on identifying the lead supervisory authority (LSA), which clarify the conditions under which controllers and processors can benefit from the One-Stop-Shop mechanism (OSS), the European Commission published a proposal for the GDPR Procedural Regulation.

This future regulation will lay down additional procedural rules relating to the enforcement of the GDPR, and seeks to harmonize and reinforce the application of data protection rules across the Member States through an enhanced OSS. As part of the legislative process, the EDPB and the European Data Protection Supervisor (EDPS) published on 19 September a joint opinion on the draft GDPR Procedural Regulation outlining suggested changes to the existing draft.[1]

This article aims to provide some insights regarding the OSS and the future GDPR enforcement rules that will bind all EU supervisory authorities.

> The proposal specifies rules for the involvement of complainants in the procedure.

What is the OSS and which entities can benefit from it?

The OSS allows controllers and processors established in the EEA to deal with a single LSA. The LSA will be the sole interlocutor for the cross-border processing carried out by the controller or processor. Organizations wishing to benefit from this mechanism must fulfil two criteria:

1. be established in the EEA and
2. engage in cross-border processing of personal data.

On this basis, they must conduct an assessment to determine the location of their "main establishment", following which, the LSA will be the supervisory authority of the Member State where their main establishment is located.

What is cross-border processing of personal data?

The term "processing" is very broad and includes any operation or set of operations which is performed on personal data or on sets of personal data (including simply collecting, storing or deleting those data). Identifying the LSA is only relevant where a controller or processor is carrying out "cross-border processing of personal data", which can happen in two scenarios:

- the controller or processor has more than one establishment in the EU (at least in two Member States) and the processing of personal data takes place in the context of the activities of these establishments; or
- the controller or processor has one establishment in the EEA, but the processing of personal data substantially affects or is likely to affect data subjects in more than one Member State.

In the second scenario, where the processor or controller has a single establishment in the EEA, the processing at stake must "substantially affect or [be] likely to affect data subjects in more than one Member State". The EDPB Guidelines further delve into this condition, and provide various examples, such as processing which causes, or is likely to cause, damage, loss or distress to individuals, or processing which leaves individuals open to discrimination or unfair treatment.

Which activities are included?

Which processing activities are considered to "substantially affect or [be] likely to affect data subjects in other Member States"?

The GDPR does not clarify which processing activities are deemed to substantially affect data subjects in other Member States. The Guidelines, however, explain that the concept of "substantially affecting data subjects" is aimed at preventing all processing activities where the controller or processor have a single establishment in the EEA, from falling within the scope of the definition of "cross-border processing". For data processing to affect an individual, the EDPB considers that processing "must have some form of impact" on the data subjects, which will be subject to a case-by-case basis assessment.

In the Guidelines, the EDPB sets out a non-exhaustive list of examples of types of processing which meet the threshold of having "some form of impact". This is the case, for example, where processing causes, or is likely to cause, damage, loss or distress to individuals, where it has an actual effect in terms of limiting rights or denying an opportunity, or where it has unlikely, unanticipated or unwanted consequences for the individuals.

Identifying the main establishment

In relation to a controller with more than one establishment in the EEA, its main establishment would be the place of its central administration in the EEA, unless the decisions on the purpose and means of the processing of personal data are taken in another establishment which has the power to have such

decisions implemented.

In relation to a processor with more than one establishment in the EEA, the main establishment would be the place of its central administration in the EEA, or (if the processor has no central administration in the EEA), the establishment of the processor in the EEA where the main processing activities take place.

It is important to consider that the mere presence and use of technical means and technologies for processing personal data or processing activities in the EEA does not constitute in itself a main establishment.

Criteria determining 'main establishment'

The EDPB Guidelines outline a non-exhaustive list of factors to determine the location of a controller's main establishment in the EEA, the most relevant being:

- the establishment where the decisions about the purpose and means of the processing are given final "sign off";
- the establishment where the decisions about business activities that involve data processing are made;
- the establishment where the power to have decisions implemented effectively lies;
- the establishment where the director with overall management responsibility for the cross-border processing is located; and
- the establishment where the controller or processor is registered as a company (if in a single territory).

It is important to note that a supervisory authority may challenge an organization's decision to appoint a LSA.

What is the role of a lead supervisory authority?

The LSA is the authority primarily responsible for dealing with cross-border data processing activities, for example, to supervise complaints from data subjects as well as carrying out investigation procedures and enforcement actions.

Being under the supervision of one single supervisory authority in the EEA can present significant advantages with respect to various compliance duties under the GDPR. For example, the GDPR introduced the requirement for a personal data breach to be notified to the LSA in the event of a cross-border breach.

However, in some cross-border processing scenarios, several LSAs can be involved. In this regard, the EDPB has brought an interesting clarification in the last version of the Guidelines, in relation to joint-controllers. Since the GDPR does not address this situation, the EDPB clarifies that the main establishment of one joint-controller cannot be considered as the main establishment of both joint-controllers. Therefore, in this instance, each joint-controller can be supervised by its own LSA.

When can several lead supervisory authorities be competent?

Depending on the processing role of the establishment(s) in question, several LSAs may be competent:

- for establishments acting as separate controllers: a multinational company with separate decision-making centres in the EEA acting as separate controllers can have more than one LSA;
- for establishments acting as joint-controllers: the GDPR does not address this situation. The EDPB introduced an important clarification in its final version of the guidelines, which is that the main establishment of one joint-controller cannot be considered as the main establishment of both joint-controllers. Therefore, in this instance, each joint-controller can be supervised by its own LSA; and
- for an establishment acting as processor: very often, one or more controller(s) will be involved in the processing together with the processor. In this case, the LSA will be the one competent to act as the lead for the controller, which means that multiple LSAs can be involved. The supervisory authority of the processor will be a "supervisory authority concerned".

Are there limits to the OSS?

Yes, for example, in the case of "local data processing activities", supervisory authorities will respect each other's competence to deal with data processing activity on a local basis. In this case, the OSS does not apply.

In addition to this, it is important to highlight that having appointed a LSA does not prevent other supervisory authorities from assuming jurisdiction over matters concerning individuals residing within their territories. This is in accordance with the principles of mutual assistance (art. 61 GDPR), and joint operations of supervisory authorities (art. 62 GDPR), whereby a LSA can allow a concerned supervisory authority to handle the case, where such concerned authority informed the LSA in the first place about this specific case.

Finally, even where the LSA decides to handle the case, the cooperation and consistency mechanisms require cooperation between the LSA, and the other concerned authority(/ies) to reach consensus over the matter. Where the supervisory authorities are unable to reach a consensus in a cross-border case, the GDPR provides for a dispute resolution mechanism, which requires the ultimate intervention of the EDPB to decide on the case, with a view to ensure a consistent interpretation of the GDPR.

How does the draft GDPR Procedural Regulation address the OSS?

On 4 July 2023, the European Commission published the draft GDPR Procedural Regulation, which harmonizes some procedural matters in cross-border cases. Although the OSS mechanism remains unchanged, the proposal complements the GDPR by detailing several procedural rules for the GDPR cross-border enforcement.

This proposal acknowledges the existence of different national procedural rules that hinder the smooth and effective functioning of the GDPR's cooperation and dispute resolution mechanisms in cross-border cases. To solve this issue, the proposal specifies rules for the involvement of complainants in the procedure and for the rejection of complaints in cross-border cases and clarifies the roles of the LSA and those of the authority with which the complaint was lodged. Moreover, the proposal provides the parties under investigation with the right to be heard at key stages in the procedure, including during dispute resolution by the EDPB. Finally, it establishes a framework for all supervisory authorities to provide

their views early in the investigation procedure.

Joint opinion by EDPB and EDPS

In their joint opinion on the draft GDPR Procedural Regulation, the EDPB and the EDPS express their views and concerns with respect to the various procedural elements laid down in the draft regulation. As an example, they suggest that the supervisory authority with which the complaint was lodged should be able to make inquiries with the relevant parties with a view to preliminarily establish competence. This means that the supervisory authorities would be entitled to assess whether the matter involves cross-border data processing or if it is a purely local matter.

According to the EDPB and EDPS, the person who filed the complaint should be able to express their thoughts on the preliminary findings, which is not the case in the existing draft. Moreover, they suggest that the competent supervisory authorities are informed of the views received from the parties under investigation before the revised draft decision is circulated by the LSA, to avoid the risk that the final decision includes elements that were not brought to the attention of the competent authorities.

What steps should companies be taking?

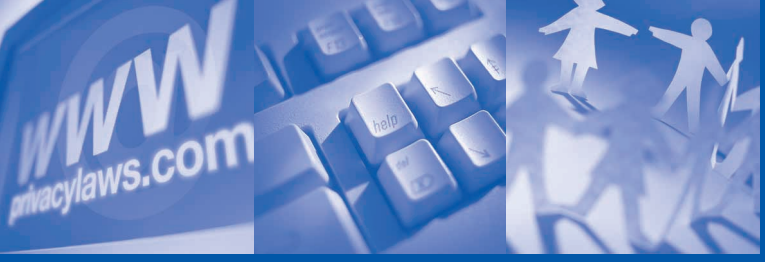
1. Companies that engage in cross-border data processing in the context of the activities of their EEA establishments should consider the roles of their entities in the EEA and determine which is their main establishment.
2. Some companies may decide to formally appoint their LSA, to align with their compliance strategy.
3. In compliance with the accountability principle, the reasons for appointing one LSA should be documented in an objective assessment, especially if the company finds itself in a borderline situation, where several supervisory authorities may consider themselves as the lead.
4. This assessment should consider all relevant factors, notably whether the establishment has the authority to implement decisions about the processing and to be liable for the processing, including having sufficient assets.[2]

AUTHORS

Patrick van Eecke is a Partner, Loriane Sangaré-Vayssac an Associate, and Enrique Capdevila a special Counsel at Cooley in Brussels.
Emails: pvaneecke@cooley.com
lsangarevayssac@cooley.com
ecapdevila@cooley.com

REFERENCES

1 edpb.europa.eu/system/files/2023-09/edpb_edps_jointopinion_202301_proceduralrules_ec_en.pdf
2 EDPB Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority; 10 October 2022, section 36



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Data protection enforcement trends in Germany

By **Julia Garbaciok** and **Katharina A. Weimer** of Fieldfisher.

In Germany there have been interesting recent decisions and trends across the country. In this article we discuss the latest news on e-marketing consent rules, and give an overview on recent developments in German employee data protection law, as well as a few highlights relating to data subjects' access rights requests.

Continued on p.3

Creating an AI governance framework: US and EU take steps to lead

The EU is finalising its AI Act while the US adopts a Presidential Executive Order on AI and creates an Artificial Intelligence Safety Institute. How are companies preparing? By **Laura Linkomies**.

The EU is still in the middle of the Trilogue process between the European Parliament, the European Council, and the European Commission. In October, they agreed on wording addressing important classification rules for high-risk artificial intelligence (AI) systems, but there are still other aspects to be finalised. There will be a certification regime for high-risk AI systems, and the Commission now

Continued on p.6

Issue 186 **DECEMBER 2023**

INTERNATIONAL report

ISSUE NO 186 DECEMBER 2023

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Julia Garbaciok and Katharina A. Weimer
Fieldfisher, Germany
Professor Graham Greenleaf
UNSW, Australia
Nana Botchorichvili
IDEA Avocats, France
David van Boven
Privacy Lawyer, the Netherlands
Patrick van Eecke, Loriane Sangaré-Vayssac and Enrique Capdevila
Cooley, Belgium
Yaron Dori, Megan Crowley and Diana Lee
Covington, US
Uche Val Obi San
Alliance Law Firm, Nigeria
Abigail Dubiniecki
Privacy Consultant, Canada

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Keeping up with AI is a challenge

There are so many privacy developments in AI governance. This issue will give you a good insight into some of the most recent news. The US Executive Order pushes the US to the lead in AI governance (p.1 and p.8) as the EU, with its complex decision-taking structure, has been delayed in adopting its AI Act. EU DPAs are alert and conduct their own investigations on AI but also unite at the European Data Protection Board to construct common positions. There is an important role for lawyers and DPOs now that market practices are developing. Privacy must be baked into products but also into organisations' AI governance, as our correspondent says.

But thoughtful public policy decisions are difficult to make when we do not fully understand the opportunities and risks with using AI, nor the impact on society as a whole.

Specifically working on privacy and new technologies is the International Working Group on Data Protection in Technology (the Berlin Group) which issues working papers on specific themes. The German-led group provided an update at the DPAs' Global Privacy Assembly in Bermuda, saying it works especially closely with the UK ICO and France's CNIL to develop future technology monitoring so that DPAs can issue privacy-friendly advice at an early stage of development of these technologies (www.bfdi.bund.de/EN/Fachthemen/Inhalte/Europa-Internationales/Berlin-Group.html).

In Bermuda, views were exchanged on the new EU-US Data Privacy Framework, which will inevitably face challenges (p.14), as well as enforcement cooperation, AI, risk based approaches and more (p.26).

We welcome your speaker offers in the first half of December for PL&B's 37th Annual Conference 1-3 July 2024 at St. John's College, Cambridge www.privacylaws.com/events-gateway/events/2024ic37/

As this is the last edition for 2023, I would like to thank you, our loyal readers, for your support and feedback (more needed though!). We are privileged to work with so many talented people, especially our *PL&B* Correspondents.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 180+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative 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 and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. 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.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked at least 7 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

> "An indispensable resource for anyone who has a serious interest in privacy, combining latest news with thoughtful commentary and analysis."
>
> **Richard Cumbley, Partner, Linklaters**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the current Data Protection and Digital Information Bill, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

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