DIGITALEUROPE

2 DECEMBER 2022

# Pursuing more harmonised and consistent GDPR enforcement: LSAs and single contact points

## Executive summary

In November 2022, the European Data Protection Board (EDPB) issued draft updates of two sets of Guidelines,[1] thereby adding information about the role or potential exclusion of the lead supervisory authority (LSA). DIGITALEUROPE welcomes the reflection on pursuing harmonised and consistent enforcement.[2] Importantly, a clear structure to the one-stop-shop (OSS) mechanism is key to help companies cooperate efficiently with supervisory authorities (SAs) and to avoid conflicting decisions.[3]

This paper makes recommendations to ensure the LSA's efficient and prompt identification. We notably recommend that:

- The controller, who has a duty to cooperate with SAs, should be able to rely on a single point of contact, without exceptions that would hinder a prompt notification of data breaches or smooth cooperation.
- The OSS mechanism can be used to avoid every single authority from having to be simultaneously notified of a data breach or competing for enforcement.
- Joint controllership agreements and the appointment of a representative should serve and be recognised as clear indicators to identify the LSA.

[1] Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority and Guidelines 9/2022 on personal data breach notification under GDPR.

[2] Last October 2021 we hosted a panel discussion on this topic, available at https://www.digitaleurope.org/events/gdpr-next-stop-for-the-one-stop-shop/. We also participated in the EDPS conference on effective enforcement in June 2022.

[3] See also p. 2 of our position paper *Two years of GDPR: A report from the digital industry*, available at https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2020/06/DIGITALEUROPE_Two-years-of-GDPR_A-report-from-the-digital-industry.pdf.

**DIGITALEUROPE**
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

# Table of contents


- Executive summary ..... 1
- Table of contents ..... 2
- Controllers' active role ..... 3

Making the assessment ..... 3

Agreeing joint controllerships ..... 3

- Keeping compliance tasks manageable ..... 4

Mandating a representative ..... 4

Purpose of the OSS mechanism ..... 5

# Controllers' active role

Art. 56 GDPR clearly places the concept of 'main establishment' at the centre of the assessment to identify the LSA. The controller should therefore not be barred from identifying one LSA, which is especially critical for time-sensitive data breach notifications or in complex joint controllership cases.

## Making the assessment

The controller's assessment of which authority is the LSA is intended to facilitate cooperation. It is a point of focus in both sets of Guidelines.

For instance, the controller's assessment is recognised as necessary for a prompt response to data breaches, particularly in time-sensitive and pressurised contexts. Indeed, in detailing procedures for notification of cross-border data breaches, the current Guidelines 9/2022 state that controllers should 'respond promptly' by having identified the LSA.[4] The Guidelines also note that LSA identification should be included in the controller's response plan.

However, the draft update to Guidelines 9/2022 adds a potential case – which could in fact become frequent – where *every single* authority needs to be notified.[5] This wording defeats the purpose of the OSS mechanism and would hinder a prompt response.

The present Guidelines 8/2022 state that: 'The controller itself identifies where its main establishment is and therefore which supervisory authority is its lead supervisory authority.'[6] It presents a list of indicators towards identifying the LSA, which revolves around business activities and decision-making powers, elements which the controller is best placed to know and take into account in its assessment.

## Agreeing joint controllerships

The controller is recognised as being the first in line to identify the LSA. In fact, identifying the LSA is the controller's responsibility. This responsibility should extend to joint controllers, as they are in a similarly advantageous position to determine the main place of establishment.

It should further be recognised that joint controllers should be allowed to identify one representative and LSA, as Art. 26 and Recital 79 GDPR make it mandatory for them to 'determine their respective responsibilities for compliance,' including the identification of a point of contact. Indeed, such a

[4] Para. 69, Guidelines 9/2022.

[5] Para. 73, ibid.

[6] Para. 24, Guidelines 8/2022.

division of responsibilities brings clarity upon which compliance can be built, in the full respect of data subject rights.

Further, a single point of contact is directly referred to in the GDPR and updates to Guidelines 8/2022 should not bar the mechanism from functioning in the case of joint controllership. While the assessment of controllers or joint controllers can be subject to SAs' scrutiny or require proof,[7] it should not be overlooked.

Last, it is the LSA's responsibility to ensure the swift and smooth cooperation with other SAs.[8] Removing the identification of a single LSA in the case of cross-border data breaches and joint controllerships will on the contrary make enforcement less harmonised.

## Keeping compliance tasks manageable

Guidelines 8/2022 state that the GDPR intends to make compliance tasks manageable, notably by identifying the right LSA.[9] Mandating a representative should facilitate communication between controllers and the LSA, and reinforce the OSS mechanism.

### Mandating a representative

Under the GDPR, the representative is given a mandate by the controller and can be designated to be addressed instead of them.[10] In this capacity, the representative should reflect the controller's intentions and serve as an indicator of the main place of establishment or central administration. As detailed above, the controller is central in identifying the LSA, as should be the representative.

In the case of joint controllership, as a clear division of responsibilities must be agreed on, **designating a common representative should not be discouraged**. A single representative would avoid hesitation and different channels of communication being opened with various authorities.

In general, weakening the role of central contact points, whether they serve to identify a representative or an LSA, would block direct communication channels and increase the cost of compliance.

[7] Paras 24 and 26, Guidelines 8/2022.

[8] Recital 119 and Art. 60 GDPR.

[9] Para. 21, Guidelines 8/2022.

[10] Art. 27 GDPR.

## Purpose of the OSS mechanism

The draft update to Guidelines 8/2022 includes a prescriptive sentence: 'Therefore, joint controllers cannot designate (amongst the establishments where decisions on the purposes and means of the processing are taken) a common main establishment for both joint controllers.'[11]

Similarly, the draft update to Guidelines 9/2022 foresees that even where a single representative has been successfully designated by the controller, it will not benefit from a single point of contact amongst the SAs.

These updates will directly result in a weakening of the OSS mechanism, leading to increased fragmentation and conflicting decisions.

By contrast, the Article 29 Working Party Guidelines previously endorsed by the EDPB allow joint controllers to designate the establishment where joint controllers have 'the power to implement decisions,' in other words a single main establishment for cross-border processing.[12] This approach should be restated and strengthened in the updated Guidelines.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

**Director for Infrastructure, Privacy and Security Policy**

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Béatrice Ericson

**Policy Officer for Privacy and Security Policy**

beatrice.ericson@digitaleurope.org / +32 490 44 35 66

[11] Para. 34, Guidelines 8/2022.

[12] Pp. 7–8, WP 244 rev.01.

## About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

# DIGITALEUROPE Membership

### Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Banco Santander, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

### National Trade Associations

**Austria:** IOÖ
**Belgium:** AGORIA
**Croatia:** Croatian Chamber of Economy
**Cyprus:** CITEA
**Czech Republic:** AAVIT
**Denmark:** DI Digital, IT BRANCHEN, Dansk Erhverv
**Estonia:** ITL
**Finland:** TIF
**France:** AFNUM, SECIMAVI, numeum
**Germany:** bitkom, ZVEI
**Greece:** SEPE
**Hungary:** IVSZ
**Ireland:** Technology Ireland
**Italy:** Anitec-Assinform
**Lithuania:** Infobalt
**Luxembourg:** APSI
**Moldova:** ATIC
**Netherlands:** NLdigital, FIAR
**Norway:** Abelia
**Poland:** KIGEIT, PIIT, ZIPSEE
**Portugal:** AGEFE
**Romania:** ANIS
**Slovakia:** ITAS
**Slovenia:** ICT Association of Slovenia at CCIS
**Spain:** Adigital, AMETIC
**Sweden:** TechSverige, Teknikföretagen
**Switzerland:** SWICO
**Turkey:** Digital Turkey Platform, ECID
**Ukraine:** IT Ukraine
**United Kingdom:** techUK