EDPB

Support Pool of Experts Programme

One-stop-shop Case Digest Legitimate interest

by Dr. TJ McIntyre

As part of the SPE programme, the EDPB may commission contractors to provide reports and tools on specific topics.
The views expressed in the deliverables are those of their authors and they do not necessarily reflect the official position of the EDPB. The EDPB does not guarantee the accuracy of the information included in the deliverables. Neither the EDPB nor any person acting on the EDPB's behalf may be held responsible for any use that may be made of the information contained in the deliverables.
Some excerpts may be redacted or removed from the deliverables as their publication would undermine the protection of legitimate interests, including, inter alia, the privacy and integrity of an individual regarding the protection of personal data in accordance with Regulation (EU) 2018/1725 and/or the commercial interests of a natural or legal person.

Document submitted in December 2025

Table of Contents

1. Scope, structure and methodology

This report analyses decisions related to legitimate interest under Article 6(1)(f) of the General Data Protection Regulation[1] ('GDPR') made by national Supervisory Authorities ('SAs') under the One-Stop-Shop ('OSS') mechanism in Article 60 GDPR and by the European Data Protection Board ('EDPB') under the dispute resolution and urgency provisions in Articles 65 and 66 GDPR. In this report, Article 60 decisions are collectively referred to as 'OSS decisions'.

These decisions offer insights into how SAs have interpreted and applied the concept of legitimate interest, individually and when cooperating with each other through the GDPR cooperation mechanism. From recording prank telephone calls,[2] to weighing users of rental scooters,[3] to tracking aircraft flights,[4] the decisions cover a wide range of situations. They are fact-dependent, unsurprisingly given the nature of legitimate interest as an open-ended and evolving legal basis,[5] and it can be difficult to generalise from them. However, despite these very different factual contexts these decisions present common issues around the types of interests which qualify as 'legitimate' and how to assess the necessity and proportionality of processing in particular contexts.

The report is structured as follows. Section 2 outlines the key provisions of Article 6(1)(f) GDPR, following the structure of EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR[6] and referring to relevant OSS decisions where these illustrate particular aspects. Section 3 then picks out and discusses patterns of decisions on particular topics and some broader themes that emerge. Section 4 concludes with overall observations on the decisions.

The decisions were taken from the EDPB register of final OSS decisions[7] and list of binding decisions.[8] For decisions of national lead supervisory authorities ('LSAs') the search engine on the EDPB website was used to identify OSS decisions which were indexed under Article 6(1)(f) GDPR. For EDPB binding decisions, all decisions tagged as relating to legal basis were included. Using these criteria, 62 OSS decisions and five EDPB binding decisions were identified and manually reviewed for relevance. The cut-off date for inclusion was 16 October 2025, and the decisions considered were adopted between December 2018 and June 2025. A small number of national SA decisions and court judgments have also been mentioned where they help to illustrate particular issues; however this report does not attempt a comprehensive survey of national approaches to legitimate interest.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[2] EDPBI:ES:OSS:D:2020:146.
[3] EDPBI:EE:OSS:D:2023:785.
[4] EDPBI:SE:OSS:D:2025:1825.
[5] Giovanni Sartor, 'Article 6', in *General Data Protection Regulation: Article-by-Article Commentary*, ed. Indra Spiecker gen Döhmann et al. (Nomos/Hart, 2023), 312.
[6] European Data Protection Board, 'Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, Version 1.0', 8 October 2024, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf.
[7] European Data Protection Board, 'Final One Stop Shop Decisions', accessed 17 October 2025, https://www.edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en.
[8] European Data Protection Board, 'Binding Decisions', accessed 21 November 2025, https://www.edpb.europa.eu/our-work-tools/consistency-findings/binding-decisions_en?page=0.

Some limits of this methodology should be noted. Due to national restrictions, the public register of OSS decisions does not include some or all of the decisions made by the SAs of Germany (Lower Saxony, Mecklenburg-Western Pomerania, North Rhine-Westphalia), Lithuania, and the Netherlands.[9] Analysis of some decisions was limited by the level of detail available. In several of these decisions the focus was on other issues so that legitimate interest was mentioned only in passing or was implicitly approved without discussion. Some decisions were heavily redacted, and in two cases only a summary of the decision was available.[10] Finally, the register of decisions does not record whether decisions have been challenged, so it is possible that some decisions may have been overturned in subsequent court actions.

2. Legitimate Interest under Article 6(1)(f) GDPR

Article 6(1)(f) GDPR provides a legal basis where 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child'. Article 6(1) goes on to provide that legitimate interest 'shall not apply to processing carried out by public authorities in the performance of their tasks'. Article 6(1)(f) GDPR therefore establishes three cumulative conditions for the processing of personal data to be lawful:

- First, the pursuit of a legitimate interest by the data controller or by a third party;
- Second, the need to process personal data for the purposes of the legitimate interests pursued ('necessity'); and
- Third, that the interests or fundamental freedoms and rights of the person concerned by the data protection do not take precedence over the legitimate interest of the controller or of a third party ('balancing test').[11]

2.1 Regulatory guidance

At the European Union level, guidance on legitimate interest was initially provided by Article 29 Working Party ('WP29') Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of the Data Protection Directive,[12] and more recently by EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR.[13] Several EDPB publications also address the application of legitimate interest in particular contexts, notably EDPB Guidelines 3/2019 on processing of personal data through video devices,[14]

[9] European Data Protection Board, 'Final One Stop Shop Decisions'.
[10] EDPBI:DENW:OSS:D:2018:2 and EDPBI:LT:OSS:D:2024:1361.
[11] Case C-252/21, *Meta Platforms and Others v Bundeskartellamt* (General terms of use of a social network), ECLI:EU:C:2023:537, para. 106.
[12] Article 29 Data Protection Working Party, 'Opinion 6/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC', 9 April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf; though it should be noted that Opinion 6/2014 was not one of the documents subsequently endorsed by the EDPB. See European Data Protection Board, 'Endorsement 1/2018', 25 May 2018, https://www.edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf.
[13] European Data Protection Board, 'Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, Version 1.0'.
[14] European Data Protection Board, 'Guidelines 3/2019 on Processing of Personal Data through Video Devices Version 2.0', 29 January 2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.

EDPB Guidelines 8/2020 on the targeting of social media users,[15] and EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models.[16]

2.2 Pursuit of a legitimate interest by the controller or by a third party

2.2.1 What is meant by 'interest'?

The GDPR differentiates between the *legal basis* for processing, the *purpose* of processing and the *legitimate interest* pursued by that processing.[17] This is exemplified by Article 13(1) GDPR which breaks out each element separately as part of the duty of transparency, requiring the controller to provide the data subject with '*the purposes of the processing* for which the personal data are intended as well as *the legal basis for the processing* [and] where the processing is based on point (f) of Article 6(1), *the legitimate interests pursued by the controller or by a third party'*.[18] EDPB Guidelines 1/2024 explain this distinction between 'purposes' and 'interests' as one of generality, explaining 'purpose' as 'the specific reason why the data are processed: the aim or intention of the data processing'.[19] An 'interest', conversely, is 'the broader stake or benefit that a controller or third party may have in engaging in a specific processing activity. For example, a controller may have an interest in promoting its products, whereas this interest may be advanced by processing personal data for direct marketing purposes'.[20]

In the OSS decisions surveyed, more sophisticated data controllers generally framed their legitimate interest assessments using these concepts and terminology. For example, in Urgent Binding Decision 1/2023 Meta provided a detailed range of interests which were further divided into sub-interests.[21] Less sophisticated controllers, however, tended to conflate these concepts or assert legitimate interest in a generic way. EDPBI:SE:OSS:D:2025:1738 provides an example. In this decision an online media firm, relying on advice from its consent management platform provider, used a cookie banner which stated that it relied on legitimate interest to process data for profiling and precise geodata of users. However when asked by the LSA to specify the legitimate interest it could not do so, nor demonstrate that any balancing test had been carried out. This decision also highlights the risks of relying on third party technical solutions for GDPR compliance, with the LSA noting that 'a controller [cannot] disclaim the responsibility to ensure that there is a legal basis for the company's personal data

[15] European Data Protection Board, 'Guidelines 8/2020 on the Targeting of Social Media Users, Version 2.1', 13 April 2021, https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf.
[16] European Data Protection Board, 'Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models', 17 December 2024, https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf.
[17] European Data Protection Board, 'Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, Version 1.0', para. 14.
[18] Emphasis added.
[19] European Data Protection Board, 'Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, Version 1.0', para. 14.
[20] European Data Protection Board, 'Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, Version 1.0', para. 14.
[21] European Data Protection Board, 'Urgent Binding Decision 01/2023 Requested by the Norwegian SA for the Ordering of Final Measures Regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR)', 27 October 2023, https://www.edpb.europa.eu/system/files/2023-12/edpb_urgentbindingdecision_202301_no_metaplatformsireland_en_0.pdf.

processing by referring to a supplier's recommendations' in finding that the controller did not have a legal basis for processing data from cookies.[22]

2.2.2 What is a 'legitimate' interest?

The GDPR does not define the term 'legitimate'. However the CJEU has recently addressed this issue in Case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*[23] ('*KNLTB*'), which concerned whether a national sports federation could have a legitimate interest in selling personal data of members (names, addresses, telephone numbers and emails) to sponsors. The CJEU rejected the proposition that a legitimate interest must have a positive legal basis to be 'provided for by law'[24] and accepted that a purely commercial interest could also constitute a legitimate interest.[25] It is interesting to compare EDPBI:ES:OSS:D:2020:146 on this point. In that case the LSA accepted (prior to the judgment in *KNLTB*) that a purely commercial interest could be a legitimate interest, but went on to stress that a purely commercial interest should be given less weight in the balancing test and should not prevail over a fundamental right.

In *KNLTB* the CJEU also held that a legitimate interest must be 'lawful'[26] in the sense of not being 'contrary to the law'.[27] EDPB Guidelines 1/2024 elaborate that an interest will not qualify if it is contrary to either EU or Member State law: for example, sending promotional emails for electronic cigarettes cannot constitute a legitimate interest as such emails are prohibited by the Tobacco Products Directive.[28] The facts of EDPBI:LT:OSS:D:2024:1361 provide another example. That decision concerned 'shadow blocking'[29] of users of an online marketplace by reducing visibility of their advertisements and posts without their knowledge. The LSA found that this could in principle serve a legitimate interest in promoting security of the platform by blocking abusive users, but that it failed the necessity and balancing tests. Since the events underlying that decision took place, shadow blocking has been prohibited by Article 17 of the Digital Services Act.[30] This decision therefore illustrates a situation where the interest pursued would now be 'contrary to the law' and incapable of constituting a legitimate interest before even reaching the necessity and balancing tests.

2.2.3 Is the interest clearly and precisely articulated?

EDPB Guidelines 1/2024 state that the interest must be 'clearly and precisely articulated' to ensure that it can be 'properly balanced against the interests or fundamental rights and freedoms of the data subject'.[31] The OSS decisions indicate that this is distinct from, but closely related to transparency: if the legitimate interest is not sufficiently clear for the purpose of the balancing test then it will not be sufficiently clear to provide adequate notice to the data subject.

[22] EDPBI:SE:OSS:D:2025:1738, 4.
[23] Case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond,* ECLI:EU:C:2024:857.
[24] Case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond,* ECLI:EU:C:2024:857, para. 39.
[25] Case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond,* ECLI:EU:C:2024:857, para. 49.
[26] Case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond,* ECLI:EU:C:2024:857, para. 40.
[27] Case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond,* ECLI:EU:C:2024:857, para. 49.
[28] European Data Protection Board, 'Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, Version 1.0', para. 18.
[29] Also known as shadow banning.
[30] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC. Article 17 of the Digital Services Act requires hosting providers to give reasons to users for restrictions imposed where material is illegal or contrary to their terms and conditions.
[31] European Data Protection Board, 'Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, Version 1.0', para. 17.

In several decisions LSAs found that a vague statement of legitimate interests would fail to establish a legal basis under Article 6 GDPR and would also breach the duty of transparency under Article 13 GDPR.[32]

Lack of specificity was one of the most common pitfalls for controllers. For example, EDPBI:BE:OSS:D:2022:325 concerned the Transparency & Consent Framework administered by IAB Europe to facilitate real time bidding for online advertising. The overall aim was to collect and process users' personal data in order to offer personalised advertisements. The LSA found that the processing purposes were 'described in general terms, with the result that it [was] not easy for users to assess to what extent the collection, dissemination and processing of their personal data are necessary for the intended purposes' so that 'the lack of specificity of the stated purposes means that the first condition for specific lawful processing is not met'.[33] For example, the LSA found that terms such as 'measure content performance' and 'apply market research to generate audience insights' provided 'little or no insight into the scope of the processing, the nature of the personal data processed or for how long the personal data processed will be retained if the user does not withdraw his consent'.[34] That decision also highlights the close links between specificity and transparency by focusing on the extent to which users could understand the purposes involved.

Binding Decision 2/2022 Meta (child Instagram users)[35] reached a similar result in relation to contact details of child users on the social media site Instagram. The context was that Meta allowed child users to switch from personal accounts to business accounts, but in doing so required them to provide either an email address or a phone number which would then be publicly available on their Instagram profile page. If the child's Instagram account was private, they would be prompted to switch to a public account as part of the switch to a business account. To justify this processing, Meta asserted two distinct interests: its own interest in 'creating, providing, supporting, and maintaining innovative products and features that enable people under the age of majority to express themselves, communicate, and engage with information and communities relevant to their interests and build community' and the interest of third parties (other Instagram users) to be able to engage with business account owners. However the EDPB found that these were 'identified and described in a vague fashion' and therefore were not sufficiently specific to 'assess whether the interests argued are real and lawful (i.e., acceptable under the law)'.[36]

2.2.4 Examples of legitimate interests

GDPR Recitals 47 to 50 provide a non-exhaustive list of situations where a controller may have a legitimate interest including: where the data subject is a client or in the service of the

[32] E.g. EDPBI:EE:OSS:D:2025:1791, EDPBI:ES:OSS:D:2020:146.
[33] EDPBI:BE:OSS:D:2022:325, paras. 446–452.
[34] EDPBI:BE:OSS:D:2022:325, para. 433.
[35] European Data Protection Board, 'Binding Decision 2/2022 on the Dispute Arisen on the Draft Decision of the Irish Supervisory Authority Regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR', 28 July 2022, https://www.edpb.europa.eu/system/files/2022-09/edpb_bindingdecision_20222_ie_sa_instagramchildusers_en.pdf.
[36] European Data Protection Board, 'Binding Decision 2/2022 on the Dispute Arisen on the Draft Decision of the Irish Supervisory Authority Regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR', para. 110.

controller,[37] fraud prevention,[38] direct marketing,[39] transfer of data within a group of undertakings,[40] ensuring network and information security,[41] and notifying a competent authority of possible criminal acts or threats to public security.[42] The NIS2 Directive expands on these by stating that a controller may have a legitimate interest in processing data under Article 6(1)(f) GDPR as part of cybersecurity information-sharing arrangements or voluntary notification of information about incidents, cyber threats and near misses.[43]

Other legislation, while not explicitly addressing Article 6(1)(f) GDPR, may also be taken into account in identifying other situations where a legitimate interest may be recognised. For example, the Sixth Anti-Money Laundering Directive ('AMLD6') provides that various individuals and bodies (such as journalists, civil society organisations and providers of anti-money laundering products) may have a 'legitimate interest' in accessing beneficial ownership information to combat money-laundering.[44] While this is not the same as 'legitimate interest' under Article 6(1)(f) GDPR, AMLD6 provides support for recognising such a legal basis.

In 2014, WP29 Opinion 6/2014 indicated that 'a broad range of interests [may qualify as legitimate], whether trivial or very compelling, straightforward or more controversial'.[45] This identified legitimate interests as including, for example, exercise of the right to freedom of expression or information, enforcement of legal claims including debt collection via out-of-court procedures, sending of unsolicited non-commercial messages for political campaigns or charitable fundraising, administration of whistle-blowing schemes, and employee monitoring for safety or management reasons.[46] Since then the CJEU has held that controllers and third parties may have a legitimate interest in matters such as the continued functioning of publicly accessible websites,[47] obtaining the personal information of a person who damaged their property to sue that person,[48] protecting the property, health and life of the co-owners of a building,[49] product improvement,[50] and assessing the creditworthiness of individuals.[51] Regulatory guidance continues to recognise legitimate interests in new contexts: for example, EDPB Opinion 28/2024 has recently stated that controllers may have a legitimate interest in

[37] GDPR, Recital 47.
[38] GDPR, Recital 47.
[39] GDPR, Recital 47.
[40] GDPR, Recital 48.
[41] GDPR, Recital 49.
[42] GDPR, Recital 50.
[43] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, Recital 121.
[44] Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849, Articles 12 to 14.
[45] Article 29 Data Protection Working Party, 'Opinion 6/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC', 24.
[46] Article 29 Data Protection Working Party, 'Opinion 6/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC', 25.
[47] Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.
[48] Case C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*, ECLI:EU:C:2017:336.
[49] Case C-708/18, *TK v Asociația de Proprietari bloc M5A-ScaraA*, ECLI:EU:C:2019:1064.
[50] Case C-252/21, *Meta Platforms and Others v Bundeskartellamt* (General terms of use of a social network), ECLI:EU:C:2023:537.
[51] Joined Cases C-26/22 and C-64/22, *SCHUFA Holding* (Libération de reliquat de dette), ECLI:EU:C:2023:958.

developing AI systems to assist users, detect fraudulent content or behaviour, or improve threat detection in information systems.[52]

Between them, this legislation, caselaw, and regulatory guidance establish a very wide range of legitimate interests, and in almost all the OSS decisions in this study the interests relied upon were ones which had already been established.[53] However a few relatively novel legitimate interests were recognised by LSAs, including rating taxi passengers to ensure driver safety,[54] preventing users banned from internet services from evading that ban,[55] and recording and sharing information about global air traffic for various third party uses.[56]

2.2.5 Societal and public interests

Article 6(1)(f) GDPR permits processing on the basis of 'the legitimate interests pursued by the controller or by *a third party'*.[57] EDPB Guidelines 1/2024 clarify this as requiring processing to be necessary and proportionate for the legitimate interests of a *specific* third party or parties, rather than general public interests.[58] The Guidelines indicate that processing in the interests of the wider community should instead normally be justified by Articles 6(1)(c) GDPR (compliance with a legal obligation) or 6(1)(e) GDPR (task carried out in the public interest).[59]

This point is illustrated by EDPBI:DEBY:OSS:D:2024:1594 in which the Worldcoin Foundation – a body seeking to establish an international identity verification and financial network based on iris scans – sought to justify processing of iris data as promoting the 'privacy of internet users in general' and 'universal access to the global economy for everyone'.[60] The LSA, however, characterised these as public interests which a private operator could not assert, notwithstanding that Worldcoin purported to operate on a non-commercial basis. The LSA also rejected the proposition that these goals could be justified as promoting the interests of Worldcoin users themselves. The LSA stressed that Article 4(10) GDPR defines 'third party' to mean 'a natural or legal person, public authority, agency or body *other than the data subject'*,[61] so that the interests of Worldcoin users (as data subjects) could not be treated as third party interests. The LSA discussed the reasoning behind this exclusion, stating that:

> A controller acting (only) in the interests of the data subject should of course not be allowed to process the data of the data subject independently of (or against) their will. Otherwise, a data controller could virtually become the custodian of the interests of the

[52] European Data Protection Board, 'Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models', para. 69.
[53] For example: assessment of creditworthiness (EDPBI:DEBE:OSS:D:2024:1282), fraud prevention (EDPBI:EE:OSS:D:2024:1404), out-of-court debt collection (EDPBI:SE:OSS:D:2025:1753), direct marketing (EDPBI:SE:OSS:D:2024:1570), facilitating third parties to enforce their legal rights against the data subject (EDPBI:IT:OSS:D:2024:1428), product improvement (EDPBI:FI:OSS:D:2022:627).
[54] EDPBI:EE:OSS:D:2025:1791.
[55] EDPBI:IE:OSS:D:2022:360.
[56] EDPBI:SE:OSS:D:2025:1753.
[57] Emphasis added.
[58] Citing Case C-252/21, *Meta Platforms and Others v Bundeskartellamt* (General terms of use of a social network), ECLI:EU:C:2023:537, para. 124 and Joined Cases C-26/22 and C-64/22, *SCHUFA Holding* (Libération de reliquat de dette), ECLI:EU:C:2023:958, para. 83.
[59] European Data Protection Board, 'Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, Version 1.0', para. 25.
[60] EDPBI:DEBY:OSS:D:2024:1594, para. 586.
[61] EDPBI:DEBY:OSS:D:2024:1594, para. 587, emphasis added.

> data subject and make decisions regarding their personal data over their head, without being able to demonstrate a (valid) reason for the data processing.[62]

Other OSS decisions, however, indicate that the wider public interest can be taken into account in determining whether third parties can assert legitimate interests. In EDPBI:SE:OSS:D:2025:1825 the data controller, Flightradar, operated a website and app which tracked the movement of aircraft worldwide, enabling users to find the real time and historical location of specific aircraft. The LSA found that this constituted the processing of personal data of the owners and pilots in some cases, particularly in relation to aircraft owned by natural persons. Flightradar sought to justify this processing as promoting the legitimate interest of third parties in monitoring global air traffic. In doing so, it provided evidence that Flightradar data was used, *inter alia*, by the aviation industry for research and development, in media reporting, and by national authorities in investigations of accidents. The LSA accepted that Flightradar could rely on the legitimate interests of third parties, saying that 'Flightradar acts … to some extent in a public interest, which may be considered to weigh relatively heavy in the assessment of whether Flightradar's interest is legitimate'.[63]

Interestingly, in that decision Flightradar also relied on the fact that police have used this flight data for criminal investigations. However the Swedish SA appears to have disregarded this point in deciding whether a legitimate interest exists, citing *Meta v. Bundeskartellamt*[64] for the proposition that 'a controller that primarily pursues an economic interest in processing of personal data cannot, as a general rule, rely on a legitimate interest in processing personal data for the purposes of preventing, detecting or prosecuting criminal offences, when this is unrelated to its commercial activities'.

This aspect of the Flightradar decision might also be seen as raising a wider point: should a controller be able to rely on the legitimate interest of a public authority as the legal basis for processing, when under Article 6(1) GDPR that public authority could not rely on legitimate interest as the legal basis for its own processing? This specific issue did not arise in any of the OSS cases, but it may be useful to compare a judgment of the Court of Noord-Nederland[65] on this point. Here the plaintiff was an individual who set up a website with livestreams from cameras in her locality covering the village centre, waterway, bridge, and harbour. These cameras also captured footage of homes, and individuals could be recognised from the livestream. The plaintiff asserted that various third party legitimate interests justified this processing of personal data, including those of the local municipality which had subsidised the cameras and used the livestreams to monitor the bridge. This was rejected by the Court of Noord-Holland, however, which held in essence that it would be illogical if the plaintiff could rely on the legitimate interest of public bodies when those bodies could not themselves assert such an interest.

2.3 Necessity of the processing

[62] EDPBI:DEBY:OSS:D:2024:1594, para. 589.
[63] EDPBI:SE:OSS:D:2025:1825, 17. See also EDPBI:DEBY:OSS:D:2024:1594 (Worldcoin) where the LSA states that '[I]f the interests of the general public pursued by the processing overlap with equally pursued specific interests of the controller or a (specific) third party, the interests of the general public may be considered in the balancing of interests to be carried out in accordance with point (f) of the first subparagraph of Article 6(1) GDPR.'
[64] Case C-252/21, *Meta Platforms and Others v Bundeskartellamt* (General terms of use of a social network), ECLI:EU:C:2023:537.
[65] Rechtbank Noord-Nederland, 22-3460, ECLI:NL:RBNNE:2025:83.

The second stage in establishing a lawful basis for processing under Article 6(1)(f) GDPR is to demonstrate that the legitimate interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter.[66] This includes considering whether processing meets the principle of data minimisation under Article 5(1)(c) GDPR.[67]

In numerous OSS decisions and one EDPB urgent binding decision it was found that processing was not necessary as there were alternatives which could achieve the legitimate interests of the controllers. For example:

- In Urgent Binding Decision 1/2023 Meta (Behavioural Advertising) the EDPB found, applying earlier decisions, that that there are realistic, less intrusive alternatives to online behavioural advertising, making the processing at stake not necessary.[68]
- In EDPBI:ES:OSS:D:2021:338 the LSA found that hotel use of guest photographs was not strictly necessary to prevent fraud, as other means such as checking surnames and room numbers or requiring signatures could be used.
- In EDPBI:DEBE:OSS:D:2022:477 the LSA determined that forcing customers to provide their phone number for customer service purposes was not necessary, as a less intrusive and equally effective means of communication (contacting customers by email) was available. In particular it was not necessary to collect phone numbers to query suspected fraud with the customer as the controller could safeguard its interests by blocking the suspect transaction.
- In EDPBI:CZ:OSS:D:2019:56 publication of a debtor's details on the internet was found not necessary to meet the creditor's legitimate interest in payment, as legal remedies to enforce payment could have been used instead.

EDPBI:DEBY:OSS:D:2024:1594 had one of the most detailed assessments of necessity in the OSS decisions with a close examination of the technical architecture chosen by the data controller. This concerned the Worldcoin Foundation which sought to use iris scans as the basis for an internet-wide system to uniquely identify users (see also section 2.2.5, above). Worldcoin sought to retain biometric iris codes even after account closure for various reasons, one of which was to ensure that users could not avoid service provider bans by deleting their biometric details and then re-registering with a new identity. The LSA accepted that in principle online services had a legitimate interest in 'protecting the integrity of their online spaces' by permanent blocking of access in some cases.[69] Nevertheless, this could not justify retention of iris codes of all users who closed their accounts. The LSA noted that under this approach 'every user is placed under general suspicion of being blocked … without the actual existence of such a block'.[70] Instead, the LSA noted, Worldcoin could contact connected services to see if a block

[66] Joined Cases C-26/22 and C-64/22, *SCHUFA Holding* (Libération de reliquat de dette), ECLI:EU:C:2023:958, para. 77.
[67] Joined Cases C-26/22 and C-64/22, *SCHUFA Holding* (Libération de reliquat de dette), ECLI:EU:C:2023:958, para. 77.
[68] European Data Protection Board, 'Urgent Binding Decision 01/2023 Requested by the Norwegian SA for the Ordering of Final Measures Regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR)'.
[69] EDPBI:DEBY:OSS:D:2024:1594, para. 607.
[70] EDPBI:DEBY:OSS:D:2024:1594, para. 605.

existed for a particular user; if not, there would be no justification to retain the user biometrics on closure of the account.[71]

Binding Decision 2/2022[72] Meta (Instagram Child Users) should also be mentioned. Here the EDPB found that publication of contact details of child business account users was not necessary to achieve any relevant legitimate interests of Meta and third parties, as it was possible to contact business users through direct messaging on Instagram, rather than by e-mail or phone (and many business users indicated that they preferred this route). The LSA had taken the view that 'the publication of the contact details of minors may have been necessary in some cases [i.e. for] business account users who wished to be publicly contactable by email or phone'.[73] However the EDPB noted that '[t]he benefits that such processing may bring to … the child business account owners … are not a relevant element for the assessment of necessity of the processing. Article 6(1)(f) GDPR is clear when it states that the legitimate interests are those of the controller or of a third party (and not those of the data subject)'. [74] It would seem to follow that if the necessity asserted is the need to implement the wishes of the data subject then the appropriate legal basis should instead be consent.

2.4 Balancing test

The third condition for reliance on legitimate interest as a legal basis under Article 6(1)(f) GDPR is that the legitimate interest in question is not overridden by the interests or fundamental rights and freedoms of the data subject. This requires the controller to carry out a balancing exercise which, according to EDPB Guidelines 1/2024, should identify and describe:

1) The data subjects' interests, fundamental rights and freedoms.
2) The impact of the processing on data subjects, including:
   a) The nature of the data to be processed,
   b) The context of the processing, and
   c) Any further consequences of the processing.
3) The reasonable expectations of the data subject.
4) The final balancing of opposing rights and interests, including the possibility of further mitigating measures.[75]

The following sections take these elements individually and discuss OSS decisions relevant to each one.

[71] Compare EDPBI:PL:OSS:D:2020:194. (Retention by bank of customer details for six years after customer closed closed; bank could not rely on a theoretically possible future claim when there were no circumstances indicating a claim might be made.)
[72] European Data Protection Board, 'Binding Decision 2/2022 on the Dispute Arisen on the Draft Decision of the Irish Supervisory Authority Regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR'.
[73] European Data Protection Board, 'Binding Decision 2/2022 on the Dispute Arisen on the Draft Decision of the Irish Supervisory Authority Regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR', para. 115.
[74] European Data Protection Board, 'Binding Decision 2/2022 on the Dispute Arisen on the Draft Decision of the Irish Supervisory Authority Regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR', para. 116. Compare EDPBI:DEBY:OSS:D:2024:1594 (Worldcoin) on this point, as quoted in section 2.2.5 above.
[75] European Data Protection Board, 'Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, Version 1.0', para. 32.

2.4.1 Data subjects' interests, fundamental rights and freedoms.

EDPB Guidelines 1/2024 note that the balancing test must take into account 'interests' of the data subject (including financial, social and personal interests), not merely fundamental rights and freedoms.[76] The OSS decisions surveyed tended to take an expansive view of these wider interests. For example, EDPBI:CZ:OSS:D:2019:56 noted that online publication of details of individuals' debts could lead to 'an adverse impact on the rights of these persons in both their personal life and work life. Such information can lead to social exclusion of such persons and their family members, loss of employment and other negative implication'.[77] Similarly EDPBI:EE:OSS:D:2025:1791 took into account the risk that a passenger might be refused taxi rides because of a negative driver review.

EDPBI:DEBY:OSS:D:2024:1594 was notable in recognising that data subjects may have 'a right to lie' which should be taken into account in assessing processing. This decision concerned biometric iris scanning promoted by the Worldcoin Foundation, which was intended to form part of a secure global identification system which would tie users to a single online identity. The LSA noted that this was concerning because it did not allow data subjects to conceal information in response to an unjustified or illegal demand:

> A simple example of a practical lie could be if one is for example, coerced into providing his or phone number in an online shop. Because one does not want to receive unsolicited advertising calls, one gives a wrong phone number. However, there are not only situations in which the possibility to lie is practical, but rather necessary or even vital. For example, in (German) labour law there is also a right to lie on particularly intimate questions of the potential future employer which are unrelated to work, such as pregnancy, illness, trade union membership, religious affiliation, existence of debts, etc. The possibility to lie about one's identity and not being (simple) to single out is not only important for prisoners of war and political dissidents, but can [be] relevant to each and every one. However, biometric data deprives a person of this possibility.[78]

2.4.2 Impact of the processing on data subjects

EDPBI:DEBY:OSS:D:2024:1594 (Worldcoin) was interesting in its discussion of the impact which its proposed biometric identification system might have on data subjects. The LSA noted that, assuming that the system worked as described, the biometric data would make the individual permanently identifiable with a profile permanently attached to them. This, according to the LSA, amounted to a complete loss of power of the data subjects over their biometric data, and therefore a loss of informational self-determination under Articles 1 and 2(1) of the Basic Law of the Federal Republic of Germany.

The LSA also stressed how failure modes of the system might affect data subjects. The LSA noted that biometric authentication is a probabilistic procedure that will always have false positive and false negative rates: in the event that the Worldcoin system succeeded in its aim of becoming a global authentication method then false negatives (failure to recognise a user who is already registered) could cause users to lose access to essential services, resulting in social and economic disadvantage. Similarly, the scale of the system (and the fact that iris codes

[76] European Data Protection Board, 'Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, Version 1.0', paras 36–38.
[77] EDPBI:CZ:OSS:D:2019:56, 4.
[78] EDPBI:DEBY:OSS:D:2024:1594, para. 540.

were processed in a central database) meant that if the system were to be compromised by a third party 'such as a public authority or a malicious attacker' then that third party would have access to all collected biometric identifiers creating 'risks of magnitude that cannot yet be estimated'.[79]

2.4.3 Reasonable expectations of the data subject

The reasonable expectations of the data subject are central to the balancing test. Recital 47 GDPR states that assessment of legitimate interests should take into account 'the reasonable expectations of data subjects based on their relationship with the controller', and this has also been emphasised by the CJEU in Case C-708 *TK v Asociaţia de Proprietari bloc M5A-ScaraA*[80] and Case C-252/21 *Meta*.[81]

The issue of reasonable expectations is closely related to the duty of transparency under Articles 13 and 14 GDPR, and in several decisions failure to meet the requirements of those articles meant that processing failed to meet the balancing test under Article 6(1)(f) GDPR. For example, in EDPBI:FR:OSS:D:2024:1257 the data controller had a chain of mobile phone stores across France and Belgium which it advertised to consumers by phone calls and SMS messages. It purchased these consumer contact details from data brokers; however these brokers had not indicated to the data subjects at the time of collecting the data with whom their data could be shared. The French SA found that as a result of this failure the data subjects could not reasonably expect to receive commercial prospecting offers from this company, and therefore the controller could not rely on legitimate interest as a legal basis.

Some decisions, however, permitted a controller to rely on legitimate interest even though they had not met the transparency requirements of Article 13 GDPR. In EDPBI:SE:OSS:D:2022:506 a company forwarded details of orders placed on its website to a third party fraud prevention service, including the customer's name, email address, IP address, telephone number, number of items purchased and value of the transaction. However the website merely indicated that information provided during ordering could be shared with 'external resources' which was not sufficiently specific to meet the requirement of Article 13(1)(e) GDPR to inform the data subject of the recipient (the actual provider) or the categories of recipients (anti-fraud service providers) who would receive the personal data. Nevertheless, the Swedish SA accepted that this type of processing was something which a data subject could reasonably expect when making a credit purchase on invoice, describing the failure to provide this information as a minor deficiency. The Swedish SA therefore found that the complainant's interests or fundamental rights and freedoms did not outweigh the company's legitimate interests for the processing under Article 6(1)(f) GDPR. This illustrates the point made in EDPB Guidelines 1/2024 that '[r]easonable expectations do not necessarily depend on the information provided to data subjects'.[82]

[79] EDPBI:DEBY:OSS:D:2024:1594, para. 549.
[80] Case C-708/18, *TK v Asociaţia de Proprietari bloc M5A-ScaraA*, ECLI:EU:C:2019:1064, para. 58.
[81] Case C-252/21, *Meta Platforms and Others v Bundeskartellamt* (General terms of use of a social network), ECLI:EU:C:2023:537.
[82] European Data Protection Board, 'Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, Version 1.0', para. 53. See also EDPBI:DEBB:OSS:D:2020:145 finding that port scanning of visitors to a website could was necessary and proportionate in the legitimate interest of the site owner, notwithstanding that the privacy statement did not explain that this would be done.

The fact that something is common practice in a particular sector will not necessarily show that it can be reasonably expected by data subjects. In EDPBI:BE:OSS:D:2020:200 a social networking service was investigated for the way in which it periodically accessed users' contacts for the purpose of identifying those who already used the service and sending invitations to others to join the service. Details of these contacts were held by the service for three months after closure of the user's account, unless the user stopped synchronising their address book in the meantime.[83] The controller argued that non-users should reasonably expect that their contact details might be uploaded to a social network service, pointing out that contacts were similarly uploaded by providers such as WhatsApp, Gmail, and LinkedIn as well as by operating systems such as Android, iOS, and Windows. The Belgian SA, however, took the view that the practices of those other services were not relevant to this case, and that the requirement of a proper legal basis for the processing of data of non-users applied to all service providers. While the discussion of this issue in the decision is quite short, the decision nevertheless seems to highlight two points. First, technically similar processing of data (large scale uploading of contacts) will not determine reasonable expectations where the purpose of the processing is different (users uploading for own use rather than services uploading to expand their userbase). Second, the fact that a practice is common amongst other providers should not be taken to mean that it is lawful.

EDPBI:CZ:OSS:D:2022:1278 emphasises the importance of the relationship between the data subject and the controller. In that case the data controller was a provider of anti-virus software which shared pseudonymised information on approximately 100 million users (including web browsing histories) with another company in its corporate group for statistical analysis and onward sale. The Czech SA found that users could not have expected such processing; based on the information provided by the controller users could expect, at most, that anonymised data might be transferred. It accepted that an average user would be aware of controllers using collected data for statistical purposes, but found that these expectations related to the operation or improvement of the controller's own anti-virus software and did not envisage processing the data for 'trend analytics' or disclosure to a third party. In reaching this finding the Czech SA stressed the importance of the relationship between users and the controller, relying on the fact that the main reason why users acquire anti-virus software is to protect their data and their privacy and that the controller marketed its products on these grounds. Interestingly, the Czech SA also considered the significant public outcry after the data sharing emerged as evidence that users were surprised by and could not have reasonably anticipated the transfer of data.

The decision in EDPBI:LT:OSS:D:2024:1361 illustrates that, almost by definition, a deceptive business practice is unlikely to be within the reasonable expectation of the data subject. Here the controller was an online second hand clothing marketplace which was found to have 'shadow blocked' a number of users alleged to have violated the conditions of the site by restricting the visibility of their posts without their knowledge. The controller stated that this was carried out on the legal basis of legitimate interest. The LSA accepted that the interests pursued by the controller (ensuring the security of the platform and users) were legitimate, but found that the shadow blocking was neither necessary nor proportionate when these interests could be achieved by less intrusive measures. In particular the LSA found the shadow blocking failed the balancing test under Article 6(1)(f) as it could not be expected by the data subject, and had a disproportionately negative impact on their interests and fundamental rights.

[83] Contrary to the position taken in Opinion 6/2014, which stated that a 'compare and forget' approach must be used in which contact details are deleted immediately after the service checks if a contact is already a user. See Article 29 Data Protection Working Party, 'Opinion 6/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC', 67.

That LSA decision is, unfortunately, available in summary form only. However that decision was subsequently affirmed by the Lithuanian Regional Administrative Court in a judgment which should be mentioned for its elaboration on the interaction between transparency, reasonable expectations, and legitimate interest:

> The essence of shadow block[ing], i.e. the deliberate non-disclosure of information to the user, goes contrary to the principles of GDPR, in particular the principle of lawfulness. The user to whom such measure is applied is not given any real opportunity to understand that his or her account has been restricted, let alone exercise his or her rights (such as the right to access data, the right to request their deletion or the right to object to data processing).
>
> Such a secret and disproportionate effect infringes the rights of the data subject and makes it difficult to defend his or her interests. This is particularly relevant when the person is not even provided with information about the specific violation he or she is accused of. The data subject has the right to know what actions of his or hers constitute an infringement in order to be able to stop the potentially unlawful activity or exercise the right of defence.[84]

2.4.4 Final balancing, including further mitigating measures

EDPBI:EE:OSS:D:2025:1791 provides an example of building in further mitigating measures as part of a legitimate impact assessment. This decision concerned a ride-hailing company which had implemented driver ratings of passengers without an adequate legal basis and with limited transparency as to how these ratings operated. The data controller reworked its practices and legitimate impact assessment, with input from the LSA, to address these issues. As finalised, the revised system had significant changes including:

- Detailed explanation of the rating process in the privacy notice.
- Introducing a right to challenge ratings
- In-app features to inform passengers about rating calculations, retention period for ratings, consequences of poor ratings, and rights to challenge ratings.
- Clarification that drivers see the average passenger rating before deciding whether to accept a fare.
- Restrictions on the employees who could view ratings.
- Limiting the period during which drivers could view the average rating of a passenger.
- Clarifying how ratings operate to bring about automated account suspensions, and in-app features to require human intervention and manual review of suspensions.

Following these changes, the LSA concluded that the controller could rely on Article 6(1)(f) GDPR to process passenger ratings.[85]

[84] Lithuanian Regional Administrative Court, administrative case No. eI3-1348-428/2025, judgment of 22 May 2025, available in English summary at https://administracinis.teismas.lt/en/the-court-the-state-data-protection-inspectorate-lawfully-and-reasonably-found-that-uab-vinted-has-violated-gdpr-regarding-the-processing-of-personal-data/1995.

[85] Given the cooperative approach taken by the controller, the LSA imposed a reprimand rather than administrative fine. In explaining this decision the LSA also identified procedural issues making it difficult to impose fines, particularly in cross-border cases: 'It is important to note that in Estonia administrative fines are not directly applicable according to GDPR Recital 151. Instead, fines must be determined through misdemeanor

3. Themes emerging from OSS decisions

3.1 Possible differing outcomes of national assessments of legitimate interest

The context-sensitive nature of legitimate interest, particularly the fact that national law is taken into account[86] at various stages of the assessment of the three cumulative conditions described above in section 2, creates the possibility that the outcome of assessments of legitimate interests will diverge between Member States depending on their national legal systems and practices. Two OSS decisions highlight the issues this may raise for controllers and LSAs.

In EDPBI:EE:OSS:D:2023:885 a Polish resident complained about an Estonian business which sold debts through a publicly accessible website. That website disclosed the complainant's full name, city and street of residence (but not house or apartment number) and the amount owed. The Estonian SA (the LSA) took the view that this disclosure would not be permitted under Estonian law on the basis of legitimate interest as it went beyond what was necessary for the sale of the debt and excessively embarrassed the debtor. In Estonia such data would be available only to logged-in users who identify themselves and confirm that they individually have a legitimate interest to see debtor's data.

However, because the controller targeted only the Polish market the Estonian SA consulted with the Polish SA to determine how these websites were treated in Poland. The Polish SA confirmed that this type of disclosure was routine in Poland, following a 2014 decision of the Supreme Administrative Court[87] which accepted that publication of debtor details online was in the legitimate interest of the data controller, that the debtor must envisage that his right to privacy may be limited by failure to repay a debt, and that the right of the creditor to repayment outweighed the right to privacy of the debtor. Otherwise, the debtor, invoking the right to protection of personal data, could effectively evade its obligation to pay the debt and consequently restrict the creditor's right to obtain the due payment. The right to privacy would also undermine the rules regarding the right to sell the debt and to take further actions in order to retrieve it.

The Estonian SA therefore dismissed the complaint on the basis that it would be excessive interference in business and freedom of competition if it were to prohibit the data controller's activities where these were common practice in Poland.

In EDPBI:EE:OSS:D:2022:384 a similar issue arose. Here, the data subject was a Spanish resident who complained that an Estonian data controller had reported details of failure to repay

proceedings, which involve additional substantive and procedural requirements. These proceedings, similar to criminal proceedings, require the DPA to prove fault on the part of the controller, which entails a higher burden of proof. This is even though the GDPR sets out a cooperation obligation on the controller. Furthermore, the procedural limitations of misdemeanor proceedings make them less effective in some cases. For instance, in Estonia, the statute of limitations for such cases is two years for infringements occurring before November 1, 2023, and three years for those occurring afterward. Given these constraints, pursuing misdemeanor proceedings in certain cross-border cases is often not a viable or efficient enforcement option.'

[86] For discussion of the extent to which national law may be taken into account, having regard to the goal of the GDPR to harmonise the law in the field of data protection, see the judgment of the German Federal Administrative Court of 29 January 2025, BVerwG 6 C 3.23, ECLI:DE:BVerwG:2025:290125U6C3.23.0.

[87] Supreme Administrative Court, decision of 21 February 2014, ref. I OSK 2463/12.

a debt to the Spanish national credit default database. The controller sought to rely on section 10 of the Estonian Data Protection Act, which permits transfer of data about defaults to third parties to assess the creditworthiness of borrowers. The Estonia SA, however, found that the controller could not rely on Estonian law to support a legitimate interest claim, citing the fact that the credit agreement contained a choice of law clause applying Spanish law.

These decisions illustrate how the outcome of assessments of legitimate interest may vary between Member States. They also point to difficulties which controllers and LSAs may face as a result. Unlike the Data Protection Directive,[88] the GDPR has no provision specifying the applicable law in relation to cross-border data processing.[89] While the OSS mechanism identifies the LSA, it does not prescribe the law that the LSA should apply. In these decisions, therefore, the Estonian SA effectively had to adopt choice of law criteria to choose whether to apply Estonian standards on reporting/publicising credit defaults or the standards of the place where the debtor was resident. This appears to raise legal certainty concerns for LSAs, who may have difficulty determining which Member State law/practice to apply in determining if a controller can rely on legitimate interest, as well as for controllers who may have to carry out multiple localised legitimate interest assessments.[90]

3.2 Retroactive reliance on legitimate interest as a legal basis

Although the EDPB has warned that legitimate interest should not serve as a 'last resort',[91] in several OSS decisions controllers effectively took this approach by seeking to rely on legitimate interest when a SA did not accept the legal basis initially relied upon. To what extent could they do so?

The dominant position in the OSS decisions was that a controller could not retroactively change the legal basis for processing in this way,[92] echoing the position taken in EDPB Guidelines 5/2020 on Consent.[93] Several decisions stressed that a change of basis to legitimate interest would prejudice individuals by undermining their right to information regarding the legitimate interests pursued and their right to object to the processing. For example, in EDPBI:ES:OSS:D:2021:338 the Spanish SA stated that:

> In the absence of information concerning the balancing test, the data subject is deprived of his or her right to know the legal basis for the processing alleged by the controller, and in particular, by referring to the legitimate interest, is deprived of his/her right to know what those legitimate interests alleged by the controller or of a third party would

[88] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 4.
[89] See Jiahong Chen, 'How the Best-Laid Plans Go Awry: The (Unsolved) Issues of Applicable Law in the General Data Protection Regulation', *International Data Privacy Law* 6, no. 4 (2016): 310–23.
[90] Compare EDPBI:DEBY:OSS:D:2024:1594 (Worldcoin) in which the Bavarian SA relied in part on the German Basic Law guarantee of informational self-determination in considering whether the Worldcoin foundation could establish a legitimate interest in a biometric identification system. On this basis, would it be appropriate to take into account national constitutional standards for those data subjects who are located in another Member State?
[91] European Data Protection Board, 'Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, Version 1.0', 2.
[92] See EDPBI:NO:OSS:D:2021:292, EDPBI:CZ:OSS:D:2022:1278, EDPBI:SE:OSS:D:2023:817, EDPBI:ES:OSS:D:2021:338.
[93] European Data Protection Board, 'Guidelines 5/2020 on Consent under Regulation 2016/679, Version 1.1', 4 May 2020, 25, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

> justify the processing without his/her consent being taken into account. Similarly, the data subject is deprived of his or her right to plead on what grounds that legitimate interest relied on by the controller could be counterbalanced by the rights or interests of the data subject. If the data subject was not given the opportunity to rely on them against the controller, any balancing carried out by the controller without taking into account the circumstances which might be invoked by the data subject who has not been allowed to do so would be vitiated by an act contrary to a mandatory rule.[94]

However EDPBI:EE:OSS:D:2025:1791 is an interesting outlier. In that case a ride-hailing company recorded taxi driver ratings of passengers, but in doing so had wrongfully relied on Article 6(1)(b) GDPR (performance of a contract). It sought to change its legal basis for this processing to legitimate interest under Article 6(1)(f) GDPR, and to do so retrospectively – keeping the existing passenger ratings. The LSA took the view that this was permitted as the prior Terms of Use/Privacy Policy, although inadequate, had referred in a general way to passenger data being processed on the basis of legitimate interest for the purposes of safety and security. The key passages from the decision are set out below:

> In the opinion of the Estonian DPA the lack of information to the data subject and the legality of the alternative legal basis are separate acts of GDPR infringement and the lack of information does not immediately mean that the alternative legal basis is unlawful … In conclusion [the controller's] personal data processing activities and the measures taken to protect the data subject rights did not fully comply with all the requirements of the GDPR at the time of the injunction, because the notification was not done correctly and the provided LIA had inconsistencies. However, this does not mean that [the controller] could not retroactively change the legal basis for data processing activities and bring its activities into compliance with the GDPR … [T]he Estonian DPA came to the conclusion that in order to continue processing personal data (as well as previously collected data) on the basis of a legitimate interest, the data controller must have (1) a properly formalized legitimate interest analysis proving that the controller has a legitimate interest in processing the personal data, and (2) necessary notifications made to the data subject about the legal basis and processing activities.
>
> The principles of legality, fairness and transparency laid down in the GDPR must be viewed as a whole, so as not to create a dangerous precedent in which the data controller can always rely on a new legal basis for previously collected data. It is therefore not an automatic right, but the data controller is obliged to justify how the legal basis applies to the data previously collected. It is the opinion of the Estonian DPA that in the end, the controller was able to provide sufficient evidence to justify the changing of the legal basis.[95]

In effect, this decision found that the data subjects were not in substance harmed by the initial choice of the wrong legal basis and the inadequate transparency, departing from the other decisions which found that the lack of information and inability to object to processing is itself a harm to the data subject.[96]

---

[94] EDPBI:ES:OSS:D:2021:338, 21.
[95] EDPBI:EE:OSS:D:2025:1791, 8-9.
[96] One might also compare the decision of the Litigation Chamber at the Belgian Data Protection Authority in matter 147/2022 of 17 October 2022, available at https://autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-147-2022.pdf, holding at para. 18 that; 'the addition of the legal basis 'legitimate interest' after the data collection has taken place, as in the present case, is not in accordance with the requirement that the legal

3.3 Overlap with ePrivacy Directive

Several of the OSS decisions highlighted issues caused by the interaction between the GDPR and the ePrivacy Directive.[97] For the purposes of this report, the interaction between the two regimes is particularly important in relation to cookies, where the ePrivacy Directive generally requires informed consent for use, excluding legitimate interest as a legal basis for their use.[98]

As is well-known, the one stop shop system under the GDPR is limited to the GDPR itself and there is no equivalent one stop shop procedure under the ePrivacy Directive.[99] In addition, enforcement of the ePrivacy Directive differs at national level, most significantly in relation to unsolicited electronic direct marketing ('spam') and access to data on terminal equipment (including cookies). Although some Member States entrust these ePrivacy rules to data protection authorities, in others enforcement is the responsibility of the telecommunications regulators and consumer protection agencies.[100] This division between GDPR and ePrivacy enforcement is particularly significant given that the ePrivacy Directive operates in some situations as a *lex specialis,* displacing GDPR requirements which would otherwise apply.[101]

This complex legal framework was reflected in some OSS decisions giving rise to both GDPR and ePrivacy issues. In EDPBI:SE:OSS:D:2025:1738, for example, the Swedish LSA found that it could not consider the legality of the storage and accessing of cookies, as this was a matter reserved to the telecommunications regulator:

> The Swedish Post and Telecom Authority is the sole competent supervisory authority over the Electronic Communications Act (2022:482), which contains specific requirements for the storage of cookies in terminal equipment or the collection of data from such equipment. However, the personal data processing that takes place after collection, such as analysis or profiling, is subject to the provisions of the GDPR, where IMY is the competent supervisory authority. Against that background, IMY's investigation has been limited to the processing of personal data that took place after

basis prior to the collection of the photos and the information about the relationship must be determined and made known to the data subject.'

[97] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws ('ePrivacy Directive').

[98] ePrivacy Directive, Article 5(3).

[99] European Data Protection Board, 'Opinion 5/2019 on the Interplay between the ePrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities', 12 March 2019, paras 79–85, https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.

[100] There does not seem to be an up-to-date list of national authorities responsible for ePrivacy and data protection enforcement but a (dated) list is available at: European Commission, 'List of Personal Data Protection Competent Authorities', 19 January 2014, https://digital-strategy.ec.europa.eu/en/library/list-personal-data-protection-competent-authorities.

[101] Article 95 and Recital 173 GDPR; Case C-654/23, Inteligo Media SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), ECLI:EU:C:2025:871.

> the data was collected and the deficiencies stated in the complaint relating to that subsequent processing.[102]

Notwithstanding that limitation, the Swedish LSA took the view that the requirement for consent under the ePrivacy Directive should be taken into account in applying the balancing test under Article 6(1)(f) to subsequent processing of data obtained from such cookies:

> IMY believes that the requirement for consent to collect data via cookies provides a particularly strong privacy protection and gives data subjects the opportunity to choose and control how their personal data is used. If the collected data is further processed at a later stage on the basis of legitimate interest as a legal basis, this specific privacy protection risks being eroded. This particular privacy protection of the data subject should therefore be considered in the balancing of interests under Article 6(1)(f).[103]

On the other hand, some LSAs who were competent to address ePrivacy issues did consider the legality of the use of cookies in final OSS decisions, notwithstanding that the OSS procedure itself does not apply to this issue. For example, in EDPBI:RO:OSS:D:2020:163 the LSA determined that a stock photography website had breached the national transposition of the ePrivacy Directive by using third-party (Google and Facebook) cookies for analytical and marketing purposes without first obtaining informed consent. Likewise, in EDPBI:FR:OSS:D:2023:697 the LSA found that an electronic scooter rental company had breached the national transposition of the ePrivacy Directive by placing cookies on user devices via the Google reCaptcha mechanism without informing users and without obtaining their consent.[104]

Finally, EDPBI:DEBB:OSS:D:2020:145 illustrates the practical difficulty resulting from the split between ePrivacy and GDPR enforcement. Here the LSA considered whether an online auction site could rely on legitimate interest as a legal basis for port-scanning the computers of visitors to the site. The decision did not, however, mention the underlying question of whether port-scanning without consent constituted 'the gaining of access to information already stored, in the terminal equipment of a subscriber or user' which would be prohibited by Article 5(3) of the ePrivacy Directive. It seems clear that in this case the siloed enforcement of the two regimes resulted in a significant point going unaddressed.

3.4 Consumer finance issues

Consumer finance was an extremely common area in the OSS decisions surveyed. Recurring topics included the lawfulness of credit checks, reporting of credit defaults, and other debt collection tactics.

3.4.1 Credit checks

[102] EDPBI:SE:OSS:D:2025:1738, 2.
[103] EDPBI:SE:OSS:D:2025:1738, 4.
[104] It should be noted that in those decisions the LSAs did not explicitly address the interaction between the OSS procedure and the ePrivacy Directive, nor the jurisdiction and choice of law issues which might arise as a result. These topics are beyond the scope of this report, but it may be useful to compare EDPBI:EE:OSS:D:2022:469 in which the Estonian LSA considered how to take account of the ePrivacy Directive in an OSS decision regarding the legality of direct marketing.

Several decisions involving the online retailer Zalando centred on when it was appropriate for an online retailer to carry out a credit check before concluding a transaction.[105] In these cases the LSA accepted that retailers had a legitimate interest in avoiding payment defaults and that it was necessary and proportionate for the retailer to do so by carrying out a credit check on the purchaser prior to conclusion of the sale, not merely after the final placing of an order. However the decisions stressed that this should be done only once a credit payment option has been selected by the customer (EDPBI:DEBE:OSS:D:2024:1282), and that there should be a safeguard against carrying out credit checks based on accidental selection of that option by the user (EDPBI:DEBE:OSS:D:2024:1280). In EDPBI:DEBE:OSS:D:2024:1280 the LSA accepted that adequate safeguards were in place when these queries happened only 'after a customer placed goods in the basket, entered his delivery and invoice address, selected in the checkout process "Purchase on invoice" and confirmed this input by clicking on the "further" button'. Likewise, in EDPBI:DEBE:OSS:D:2024:1279 a requirement to enter a social security number prior to completing a credit transaction was treated as an appropriate safeguard against accidental credit checks.

3.4.2 Reporting to credit default registries

Several decisions involved complaints about the reporting of debts to national credit default registries. Interestingly, although WP29 Opinion 6/2014 indicated that legitimate interest of the controller is generally the most appropriate legal basis for 'debt collection via out-of-court procedures'[106] – and the CJEU has since held that assessment of creditworthiness may also constitute a legitimate interest of customers of credit rating agencies[107] – there continue to be a number of cases in which controllers rely on other legal bases.[108]

In EDPBI:EE:OSS:D:2022:319, for example, the creditor had transferred information regarding a customer's unpaid debt to the Spanish ASNEF[109] payment default register, relying on three distinct bases: '(1) performance of the contract; (2) giving the complainant the opportunity to monitor his/her debts to [the creditor] (in addition to other notifications and the complainant's portal account); and (3) giving others the opportunity to process the complainant's data on the basis of a legitimate interest in order to assess the complainant's creditworthiness'.[110] The LSA rejected the argument that transmission of the information could be justified under Article 6(1)(b) GDPR (performance of the contract), and instead found that the controller must establish a legal basis under Article 6(1)(f) on legitimate interest – without, however, specifying precisely what legitimate interest may apply.

EDPBI:MT:OSS:D:2022:375 also concerned transmission of information to the Spanish ASNEF register. In this case a Maltese controller cited its own legitimate interest as creditor in securing payment and also a public interest under Article 6(1)(e) GDPR in informing potential lenders of the default. The controller also relied upon Article 20 of the Spanish Data Protection

[105] EDPBI:DEBE:OSS:D:2024:1279, EDPBI:DEBE:OSS:D:2024:1280, EDPBI:DEBE:OSS:D:2024:1282.
[106] Article 29 Data Protection Working Party, 'Opinion 6/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC', 25.
[107] Joined Cases C-26/22 and C-64/22, *SCHUFA Holding* (Libération de reliquat de dette), ECLI:EU:C:2023:958, para. 83.
[108] For a wider discussion of the legal framework surrounding credit default registries see Cătălin-Gabriel Stănescu, *EU Informal Debt-Collection Regulation: Failure by Design?* (Oxford University Press, 2025), ch. 13.
[109] Asociación Nacional de Establecimientos Financieros de Crédito.
[110] EDPBI:EE:OSS:D:2022:319, 2.

and Digital Rights Act 3/2018[111] which provides that such processing of information on credit defaults shall be presumed lawful if certain transparency criteria and safeguards for the debtor are followed (such as deletion of the record when the debt is repaid, or at most five years from the date of default). The Maltese SA, however, relied exclusively on Article 6(1)(f) GDPR to find that the creditor could assert two distinct legitimate interests: '(a) to pursue debt collection; (b) to inform the public, including financial entities and banks, about the complainant's indebtedness, which contributes to the stability of the financial system'.[112] The Maltese SA did not discuss Article 6(1)(e) GDPR, implicitly finding that this could not provide a legal basis for the transfer. Interestingly, the Maltese SA did not refer to the effect of Article 20 of the Spanish Data Protection and Digital Rights Act, although such a national provision would seem to be important in setting the boundaries of the consumer's legitimate interest. Compare the discussion in section 3.1, above, regarding how LSAs should assess legitimate interest in OSS cases when national law or practice differs between the Member States involved.

Both EDPBI:EE:OSS:D:2022:319 and EDPBI:MT:OSS:D:2022:375 indicate that the controller is obliged to carry out a detailed assessment of the legitimate interest and to consider whether or not the processing of the data is permissible in each particular case. The implication is that a blanket policy of referring all unpaid debts to a credit default registry would not be compatible with Article 6(1)(f) GDPR. EDPBI:MT:OSS:D:2022:375 also highlights the importance of complying with transparency obligations by notifying the data subject of the possibility that they could be included in a default register, particularly (as in that case) where the debts have been purchased by a third party.

3.4.3 Identifying debtors publicly

As already noted in section 3.1 above EDPBI:EE:OSS:D:2023:885 showed a split on the question of whether a creditor can publicly identify a debtor online on the basis of legitimate interest, with the Estonian SA stating that such identification would be excessive under Estonian law while the Polish SA stated that Polish law and practice favoured the rights of the creditor.

A similar issue arose in EDPBI:CZ:OSS:D:2019:56, in which the Czech SA came down in favour of a privacy protective approach. Here, the controller was a company which published information on its website and on its Facebook profile about debts owed by individuals, specifically the first letter of each debtor's first name and entire last name as well as the amount of the debt (e.g. J. Smith, €43,000). The LSA found that this information was sufficient to identify debtors in many cases. It accepted that more effective debt collection was in principle a legitimate interest which would be promoted by publication, but rejected the argument that publication was either necessary or proportionate. According to the LSA: 'In countries where the rule of law applies [debt collection must] be carried out in a way foreseen by law and not by public denunciation of the debtors', especially given that such information 'can lead to social exclusion of such persons and their family members, loss of employment and other negative implications'.[113] These concerns were compounded by the fact that the publication was not foreseeable by the data subject, and that the publication of details of the debt was not time limited.

[111] Organic Law 3/2018 of December 5 on Protection of Personal Data and Guarantee of Digital Rights (Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales).
[112] EDPBI:MT:OSS:D:2022:375, para. 30.
[113] EDPBI:CZ:OSS:D:2019:56, 3.

3.4.4 Contacting debtors

EDPBI:EE:OSS:D:2022:447 presented issues about techniques for tracking down and contacting debtors. The data subject was a Lithuanian resident who complained that a debt collection company had attempted to contact him through his mother, and had also sent his details (full name, year and month of birth) to an account on social media with a similar name to his. The company asserted a legitimate interest in enforcing its debts, and specifically in contacting debtors using data relating to them which had been collected from public sources. It said that it did not reveal the existence of the debt to third parties (though the LSA found that the name of the company made it clear to those contacted that the underlying reason was debt collection). The LSA found that the processing of personal data of family members and other close contacts of the debtor could not be based on legitimate interests. The processing was not necessary (as judicial proceedings could be taken), nor could individuals reasonably expect that their personal data would be processed in connection with the debts of a friend or a relative. As regards contact via a social media account under a similar name, the LSA appeared to accept that in principle this could be done in reliance on legitimate interest, but noted that there was a high risk of contacting the wrong person and transferring data without any legal basis.

3.5 Anti-fraud measures

The OSS decisions surveyed gave considerable latitude to controllers in relation to anti-fraud measures. In EDPBI:SE:OSS:D:2022:506 a company selling goods on invoice forwarded details of orders placed on its website to a third party fraud prevention service, including the customer's name, email address, IP address, telephone number, number of items purchased and value of the transaction. In this case the LSA accepted that this served the controller's legitimate interest in preventing fraud, that outsourcing this function was necessary in that the controller did not itself have the expertise to evaluate risk factors (such as whether the IP address of the customer indicated use of an anonymisation service, or multiple accounts sharing the same IP address), and that the balancing test weighed in favour of the controller.

In two decisions businesses which offered free trials of their services successfully asserted a legitimate interest in retaining user details to prevent abuse by users who might sign up for multiple free trials. This was the case in EDPBI:SE:OSS:D:2021:196 (a music streaming service) and EDPBI:RO:OSS:D:2020:163 (an online stock photography website). In both the LSAs accepted that there was a strong legitimate interest of the business in preventing reuse of free trials, and that keeping this data was necessary for this purpose. It should be noted that the identifiers (credit card details and email addresses respectively) were kept in cryptographically modified form rather than in plaintext.

The somewhat unusual case of EDPBI:DEBB:OSS:D:2020:145 concerned an online auction site which carried out port-scanning on computers of visitors to its site to identify potentially compromised devices (i.e. machines running remote desktop tools). The legal basis asserted was the legitimate interest of the business in prevention of fraud, and the legitimate interest of users in protecting their data from unauthorised access. The LSA accepted both interests as legitimate (without considering whether the controller could assert a legitimate interest of the data subject), and accepted that this was a necessary and proportionate measure. Surprisingly, however, it did so notwithstanding that all visitors were subject to port-scanning (the controller had claimed that it was done only in high-risk scenarios), and notwithstanding its finding that

the data protection statement did not adequately explain this and that 'such a method is not expected by an ordinary user of the website and is not intuitive'.[114]

3.6 Rental vehicle monitoring

Several OSS decisions concerned monitoring of rental vehicles, with concerns over excessive tracking of geolocation data. In EDPBI:FR:OSS:D:2022:430 a car rental company collected geolocation data on rental cars at 500m intervals, whenever the engine was turned on or off, or whenever a door was opened. This data was transmitted in real time to the company and stored for the entire duration of the commercial relationship and for three years from the date of the user's last activity. Similarly in EDPBI:FR:OSS:D:2023:697 an electronic scooter rental company collected location data from each scooter every 30 seconds while the scooter was active; this was then stored for 24 months. In both of these cases the French SA was the LSA and concluded that the collection and retention of data was excessive and beyond what was necessary to serve legitimate interests such as management of theft. The LSA stressed the sensitivity of this data, quoting the following passage from EDPB Guidelines 1/2020:

> location data is particularly revealing of the life habits of data subjects. The journeys undertaken are very characteristic in that they enable one to infer the place of work and of residence, as well as a driver's centres of interest (leisure), and may possibly reveal sensitive information such as religion through places of worship, or sexual orientation through places visited. Accordingly, the vehicle and equipment manufacturer, service provider and other data controllers should be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing.[115]

In EDPBI:EE:OSS:D:2023:785 a person who rented an electronic scooter complained that he had received a warning message after his trip saying that he had allowed another person to ride with him. It emerged that the scooters logged the weight of riders on each trip, sending an alert to users if the weight detected is more than 1.4 times the median weight of the user on previous trips. The controller relied on legitimate interests of promoting the safety of riders and third parties by deterring tandem use of the scooters. The LSA accepted that these were legitimate interests of the controller and third parties, accepted that users could reasonably anticipate that the controller would enforce the rule against tandem riding, and took the view that monitoring weight was less invasive than other methods of achieving the same goal (such as video surveillance). In reaching this conclusion the LSA also relied upon the fact that the alert was a warning only – it did not stop the scooter, or restrict the user in any other way and therefore was not in scope of Article 22 GDPR on automated processing.

4. Conclusion

The OSS database provides us with a sample of decisions in this area, but it is far from a complete picture of the operation of legitimate interest. As one would expect from the OSS system – which, by definition, is limited to cases with a cross-border component – the decisions predominantly involved electronic marketing or online consumer transactions. Notably there

[114] EDPBI:DEBB:OSS:D:2020:145, 4.
[115] European Data Protection Board, 'Guidelines 01/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications, Version 2.0', 9 March 2021, para. 63, https://www.edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf.

were no OSS decisions relating to the use of legitimate interest as a legal basis for employee monitoring[116] nor video surveillance – two areas which often raise legitimate interest questions but tend not to have the same cross-border dimension.[117]

Bearing that limitation in mind, the OSS decisions presented a wide range of factual contexts, from hairdressers requiring customers to provide a phone number for a walk-in haircut[118] to behavioural advertising affecting substantially all the population of Europe.[119] The level of analysis in each decision reflected the complexity and significance of the issues at stake, and the more detailed decisions almost always relied on the caselaw of the CJEU and in more complicated matters frequently relied on the WP29 and EDPB guidance documents summarised in section 2.1 above.

In almost every case the interest put forward by the controller was recognised as in principle legitimate, though it might not pass the subsequent necessity and balancing tests. While there had been some dispute as to whether a purely commercial interest could constitute a legitimate interest,[120] all the decisions in the dataset nevertheless recognised (or at least assumed) that such an interest could qualify. That said, controllers frequently failed in establishing that they could rely on a legitimate interest in their particular case.

First, many controllers simply failed to conduct or document a proper legitimate interests assessment before commencing processing.[121] This failure was almost always fatal to their reliance on Article 6(1)(f) GDPR, as SAs consistently emphasised that the assessment must be conducted *ex ante*, not retrospectively constructed in response to regulatory scrutiny.

Second, controllers frequently asserted legitimate interests that were too vague. Generic language such as 'measure content performance' or 'apply market research to generate audience insights' was rejected by SAs as lacking the specificity required by the GDPR.[122] The decisions make clear that the legitimate interest asserted must be precisely articulated in order to permit the necessity and balancing tests to be carried out and to provide adequate notice to the data subject to exercise their rights.

Third, the necessity test was a significant hurdle for many controllers. Even where a legitimate interest was accepted in principle, SAs frequently found that the processing went beyond what was necessary to achieve that interest. Where controllers asserted that processing was required by the technical system they had chosen, SAs were prepared to consider whether a less intrusive technical approach could be adopted.[123]

---

[116] Compare e.g. the decision of the French SA in relation to Amazon France Logistique (n°SAN-2023-021 of 27 December 2023) available at Commission nationale de l'informatique et des libertés, 'Surveillance des salariés: la CNIL sanctionne Amazon France Logistique d'une amende de 32 millions d'euros', 23 January 2024, https://www.cnil.fr/fr/surveillance-des-salaries-la-cnil-sanctionne-amazon-france-logistique-dune-amende-de-32-millions.

[117] Indeed GDPR Recital 127 envisages that 'the processing of employees' personal data in the specific employment context of a Member State' may be handled at local level by the concerned supervisory authority even where there is a cross-border element, subject to the approval of the LSA.

[118] EDPBI:NO:OSS:D:2022:501.

[119] European Data Protection Board, 'Urgent Binding Decision 01/2023 Requested by the Norwegian SA for the Ordering of Final Measures Regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR)'.

[120] Prior to the CJEU judgment in Case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*, ECLI:EU:C:2024:857.

[121] EDPBI:ES:OSS:D:2021:338, EDPBI:CZ:OSS:D:2022:1278.

[122] EDPBI:BE:OSS:D:2022:325.

[123] EDPBI:DEBY:OSS:D:2024:1594.

Finally, controllers failed the balancing test for a number of reasons but one of the most common was that processing did not respect the reasonable expectations of data subjects. These decisions generally raised transparency issues also, and in several decisions controllers were found to have breached Article 13 GDPR or Article 14 GDPR as well as failing to establish a legitimate interest.

For the most part, these decisions involved the application of well-known principles to new contexts and largely turned on their facts. However two relatively novel legal issues did arise which may merit further consideration. First, several of the consumer credit cases presented situations where national law and practice on debt collection differed between Member States. In these situations, LSAs faced what were, in effect, choice of law issues in deciding between their own law and the law of the Member State where the complainant resided. Second, in a number of cases data controllers sought to rely on legitimate interest retrospectively (to retain data which had been gathered without an appropriate legal basis), and there was some divergence between SAs as to whether this could be permitted, based on the circumstances of the case. Although not a novel point, the decisions also highlight the practical problems created by the overlapping GDPR and ePrivacy regimes and reinforce the argument that ePrivacy enforcement should be brought within the GDPR cooperation and consistency mechanism.[124]

[124] See e.g. European Data Protection Board, 'Statement on the ePrivacy Regulation and the Future Role of Supervisory Authorities and the EDPB', 19 November 2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_statement_20201119_eprivacy_regulation_en.pdf .


EDPB
European
Data Protection
Board