esquilin GmbH

esquilin GmbH | Max-Beckmann-Weg 65 | DE 65428 Rüsselsheim am Main

EDPB
Public Consultation

Guidelines 02/2026 on Anonymisation **2026-10-26**

Dear Sir and Madam

I am referring to recital 15.

Of course, the concept of data processing on behalf of a controller should not be undermined for precisely the reasons you cited. But wouldn't exceptions be permissible in light of the CJEU's SRB ruling if, although the data is personally identifiable from the controller's perspective, it is processed by the processor only in a form that precludes any unauthorized use of the data by the processor for purposes other than those intended - because the data is single-sidedly anonymous?

We frequently encounter such a scenario in practice when data is processed by a specialized service provider. Whether the service provider has access to the data depends, in these arrangements, on the scope of services. "Access" here is understood to mean the ability to actually become aware of the data - that is, to read it and further process it for its own purposes.

> The possibility of access to the content generally exists whenever the service provider's scope of services includes technical processing (common in Software as a Service, such as email services). The **SRB ruling** does not apply to such scenarios. However, if the scope of services falls short of this, the service provider typically has no access to the content of the data processed on its infrastructure or systems.
>
> This will typically be the case when the service provider merely provides infrastructure and, if applicable, an operating system and possibly additional system software, but the substantive processing is carried out in a (specialized) application controlled only by the controller.
>
> Provided that the (business) application in question is configured in such a way that the service provider cannot gain content-related knowledge of the data without the controller's involvement, an application of the SRB ruling would be conceivable; for from the service provider's perspective, the data is anonymous.
>
> **In such scenarios, the service provider cannot independently establish a personal link to the data with reasonable or lawful effort without the controller's assistance.**

> The same applies if the controller stores only encrypted data with the service provider and it appears that only the controller (or the data subjects themselves) can decrypt it.

In my view, **with the SRB ruling, the CJEU has also opened the door to certain forms of data processing on behalf of a controller that allow for practical simplifications** in the cases described - and are likely to be received favorably in the business world.

It seems important to me that the **rights and freedoms of data subjects** - particularly with regard to the protection objectives of confidentiality and integrity - **are not jeopardized.**

That leaves the protection objective of availability. Here, the service provider could certainly cause damage - at the expense of the data subjects - for example, by shutting down services or through inadequate maintenance. And without the application of the GDPR's rules on data processing, we would no longer have a direct obligation on the controller to select only reliable service providers.

This point must therefore be examined even more closely.

> According to the SRB ruling, the transfer of single-sided anonymised data required for the use of a service provider constitutes, from the controller's perspective, a separate processing activity under data protection law, which requires a legal basis under Article 6(1) GDPR. The legitimate interest is likely to be the applicable legal basis in such cases, which in turn entails high transparency requirements toward the data subjects. This means that, under the SRB's approach, the data subjects would have to be clearly informed of this when or before a service provider is engaged. Furthermore, the data subjects would even have a specific right to object in this regard.
>
> If data is made available to third parties by the controller in the course of data processing on behalf of the controller pursuant to Article 28 of the GDPR, this fact is also made transparent to the data subjects - though usually not in a particularly proactive or detailed manner. When legitimate interest is used as the legal basis, the transparency requirements go significantly beyond those applicable to data processing on behalf of the controller. However, the truly decisive point in data processing according to Art. 28 is the data subjects' lack of a right to object. In an SRB scenario, this necessarily follows from the presumed legal basis of legitimate interest.
>
> From the controller's perspective, engaging a service provider based on an SRB exemption is formally simpler; there is no need to negotiate a controller processor agreement. What remains is the requirement to identify an independent legal basis and the associated formalities and legal consequences. Assuming that legitimate interest applies as a rule, a fair balancing of interests is only possible if the recipient of the data does not pose a substantial risk to the data subjects. Here, the GDPR thus does provide a protective effect for data subjects.

However, an effective additional safeguard comes into play here. Data subjects could object to the choice of service provider. This potential for disruption should serve as a strong incentive for the controller to use only reputable service providers and to manage them appropriately with regard to data security (TOMs analogous to a well-drafted controller processor agreement). Provided this is the case and the balancing of interests has been conducted and documented in a clear and convincing manner, any objections that might nevertheless be raised would likely come to nothing, and thus would not pose a relevant practical problem for the controller.

Given these considerations, **no real deterioration in the legal position of the data subjects is apparent**, even with regard to the protection objective of availability.

In everyday business life, controller processor agreements are often perceived as an expensive bureaucratic burden, which has a rather **counterproductive effect on acceptance of the GDPR.** This is especially true when, from the perspective of the parties to the controller processor agreement, it is viewed as a mere formality. Cases where the processor cannot view the data - because it is encrypted or encapsulated by an application controlled solely by the controller (i.e., the SRB scenario) - are viewed as such. **With the SRB exemption discussed here, you could offer companies some relief.**

By the way: In practice, many companies would have far less work and fewer discussions regarding controller processor agreements if the Standard Contractual Clauses (SCCs) provided by the Commission for the single market were applied more consistently. In my experience, however, many companies are still unaware of these resources, even though they were published as early as 2021 (915/2021). Unfortunately, there are also very few supervisory authorities that actively promote this simplification. It would be a simple and effective step toward reducing bureaucracy.

My call for the application of the SRB ruling to certain forms of data processing by third parties - currently classified as “Article 28 processing” - remains unaffected by this additional concern regarding the SCCs.

Best regards

Joerg Weiß
Geschäftsführer

The text was translated with the help of AI. The actual content was created entirely by human authors.