

Data portability under the GDPR: control without ownership

Joris Bijvoets, CIPP/E | AVG Compleet B.V.

AVG Compleet knowledge base | 12 July 2026

<https://avg-compleet.nl/dataportabiliteit-onder-de-avg/>

The right to data portability (Article 20 GDPR) is often cited as the most "property-like" right in the General Data Protection Regulation. Whoever can take his data to another service provider appears to possess something he can also move. On closer reading it turns out to be something else: a delimited, procedural mobility right that strengthens the position of the data subject without conferring any power of disposal in the proprietary sense.

What Article 20 GDPR actually regulates

The text of the provision is narrowly drawn. Paragraph 1 gives the data subject the right to receive the personal data "which he or she has provided to a controller" in a structured, commonly used and machine-readable format, and to transmit those data to another controller. The right applies under three conditions: the processing is based on consent (Article 6(1)(a) or Article 9(2)(a)) or on a contract (Article 6(1)(b)), and the processing is carried out by automated means (Article 20(1)).

Paragraph 2 adds that the data subject may, where technically feasible, have the data transmitted directly from one controller to another. And paragraph 4 sets a limit: data portability shall "not adversely affect the rights and freedoms of others".

Together these elements determine the scope of the right. For the ownership question, one of them is the sharpest: source dependence.

"Provided": the core and the limits of the right

The notion "provided" is the most contested term in Article 20. In WP242 rev.01 (later endorsed by the EDPB), the Article 29 Working Party distinguished three categories:

- 1 **Actively provided data:** what the data subject himself entered in a form, account or profile.
- 2 **Observed data:** what the controller has recorded by observing the use of the service, such as location, click behaviour, listening history and search terms.
- 3 **Inferred data:** what the controller has constructed from those data, such as profiles, segments, scores and credit assessments.

According to the Working Party, categories 1 and 2 fall under "provided", and therefore under Article 20. Category 3 does not (Article 29 WP, 2017: 9-10).

That demarcation is less self-evident than it appears. The line between observed and inferred data is difficult to draw in concrete cases: is a ride history observed, and the assessment based on it inferred? Nor have the Dutch courts settled the question of scope. In the proceedings brought by platform drivers, the portability claim failed on appeal for lack of a sufficiently specified request, without the court reaching the question whether observed data fall under Article 20 (Amsterdam Court of Appeal, 4 April 2023, ECLI:NL:GHAMS:2023:804, para. 3.50, concerning Ola).

For the ownership question it is striking that even on the broadest reading (WP242), inferred data fall outside Article 20. It is precisely this delimitation that makes a comparison with property law instructive. In property law, ownership may in certain circumstances extend to newly formed things, through accession, confusion or specification (Articles 5:14-5:16 of the Dutch Civil Code), although that always depends on specific rules and is not automatic. In data portability a comparable link is absent: a data subject has no Article 20 claim to the profiles or scores constructed from his click behaviour.

Procedural requirements: structured, commonly used, machine-readable

The format requirement ("structured, commonly used, machine-readable") is, according to WP242, a minimum floor intended to enable re-use by another controller. Interoperability is the objective the guidelines have in mind, but the GDPR prescribes no specific standard or technical format (Article 29 WP, 2017: 17-18). Examples of usable open formats are CSV, XML and JSON; where a common format exists within a sector, alignment with it is the obvious course.

Recital 68 GDPR places the right in the key of the data subject's control over his own data; in practice it also lowers switching barriers between providers, an effect often linked in the literature to the prevention of lock-in. No proprietary regime is thereby created. The provision fosters competition and freedom of choice in the service of the data subject; it does not make him a merchant.

Paragraph 4: the rights of others

Ownership, too, is limited within the civil and fundamental-rights framework, for instance by Article 1 of the First Protocol to the ECHR, by abuse of rights (Article 3:13 of the Dutch Civil Code) or by tort law (Article 6:162 of the Dutch Civil Code). The difference with Article 20(4) lies in the form: the GDPR codifies the balancing against the fundamental rights of third parties within the right itself, whereas in ownership that balancing usually proceeds through general doctrines and external limitation. Article 20(4) GDPR states explicitly that the portability right may not adversely affect the rights and freedoms of others. That is of practical importance: contact lists, communications, family photographs and shared documents almost always contain data of third parties as well. WP242 points out emphatically that controllers must take that third-party position into account when transmitting data (Article 29 WP, 2017: 11-12).

The clause makes clear that data portability is a right within a fundamental-rights framework, not an exclusive right of disposal. It is a mobility right under conditions.

Four differences from ownership

When data portability is placed alongside the civil-law concept of ownership (Article 5:1 of the Dutch Civil Code), four distinctions stand out.

The first difference is source dependence. Ownership, once validly acquired, is in principle not dependent on the provenance of the thing, although defects in the acquisition may stand in its way (Articles 3:84 and 3:86 of the Dutch Civil Code). Article 20, by contrast, is permanently source-dependent: it applies only to what has been provided by the data subject. Actively, and according to WP242 also through observation, but expressly not to what the controller has inferred.

In addition, the right depends on the legal basis. Ownership exists regardless of the legal context, whereas Article 20 applies only where the processing is based on consent or contract. Where processing rests on legitimate interests, a legal obligation or a public task, for instance most processing by public authorities, the right does not apply.

A third distinction is the format requirement. Ownership is form-independent; Article 20 requires a structured, commonly used and machine-readable format that enables re-use.

Finally, third-party effect. Ownership is an absolute right that in principle operates against everyone, although it is limited by statute, the abuse-of-rights doctrine and fundamental rights. Article 20, by contrast, contains in paragraph 4 a built-in precedence for the rights and freedoms of others: a conflict clause within the right itself.

This is not technical hair-splitting. The four distinctions explain why data portability behaves more like a procedural right than like a property right in the classical sense.

Conclusion

In an earlier blog in this knowledge base I argued that personal data are not property under the GDPR (Bijvoets, 2026a). Data portability is the GDPR right that at first sight departs from that most: it feels like a transfer of something of one's own. The analysis above shows that on closer reading it is something else. Article 20 does not regulate the transferability of a proprietary right, but a delimited mobility right within a fundamental-rights framework. It strengthens the position of the data subject vis-à-vis platforms and service providers, without creating a market in personal data.

The practical consequences are considerable. A controller receiving a portability request cannot suffice with "you will get all your data". The law imposes a delimited obligation: actively provided (and according to WP242 also observed) data in a usable format, with respect for third-party positions, and only for the legal bases to which the right applies. A data subject invoking Article 20 must realise that profiles and scores created on the basis of his data fall outside the claim. And a court deciding a dispute will sooner or later face the question of the scope of "provided": a question the Dutch courts have so far left unanswered.

For the ownership discussion the picture remains unchanged: data portability offers control, not possession in the proprietary sense.

References

- 1 Article 29 Data Protection Working Party (2017) *Guidelines on the right to data portability*, WP242 rev.01, 5 April 2017 (endorsed by the European Data Protection Board, 25 May 2018). Available at: <https://ec.europa.eu/newsroom/article29/items/611233>, accessed on 11 July 2026.
- 1 Bijvoets, J. (2026a) *Persoonsgegevens zijn geen eigendom: waarom de AVG kiest voor zeggenschap* [Personal data is not property: why the GDPR opts for control]. AVG Compleet. Available at: <https://avg-compleet.nl/persoonsgegevens-zijn-geen-eigendom/>.
- 1 Dutch Civil Code, Article 5:1.
- 1 Amsterdam Court of Appeal, 4 April 2023, [ECLI:NL:GHAMS:2023:804](#) (platform drivers v Ola), para. 3.50; compare Amsterdam District Court, 11 March 2021, [ECLI:NL:RBAMS:2021:1019](#).
- 1 [Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ 2016 L 119/1, in particular Articles 6, 9 and 20 and recital 68.

This English edition corresponds to the Dutch online article published by AVG Compleet. Legal information reflects the position stated on the publication date.