

Freedom of personal data business – conflict of commercial practice and authority review

By Jalmari Männistö

Personal data processing and conducting business in an IT environment are high inseparable concepts. The GDPR and limited national statutory instruments create a walled garden in which such enterprises are free to operate within clear boundaries – or do they? A rising theme in Nordic authority and court jurisprudence is the role and weight given to a business's freedom to choose its methods of operation in relation to how they affect the protection of personal data. The question essentially is to what extent a commercial choice can justify or undermine related personal data processing.

This short article explores the topic via two recent Finnish court decisions (the Posti/OmaPosti case and the data protection fine imposed on [Verkkokauppa.com](https://www.verkkokauppa.com)), wherein the respective companies defended themselves against data protection fines on the basis that the allegedly breaching data processing was the result of legitimate commercial choices.

Legal background

While the GDPR does *not* set out to which extent a data controller's commercial choices dictate the scope of processing, this autonomy is indirectly protected through general legal principles and the broader regulatory context. Recital 4 of the GDPR explicitly recognises (in line with the broader EU fundamental rights regime) that “*the right to protection of personal data is not an absolute right*”, underlying the fact that it

must be balanced according to the principle of proportionality against other rights, such as the freedom to conduct a business. In line with later analysis, both the Finnish Constitution (Section 18) and the EU Charter of Fundamental Rights (Article 16) contain express recognitions of the freedom to conduct a business, requiring a proportionality assessment when these rights conflict. In practice, this conflict assessment is generally baked into the more clear-cut application of data protection regulation, but the broader statutes require an additional balancing exercise.

While the GDPR utilizes a risk-based approach for managing data processing, this framework focuses primarily on implementing security measures and mitigation strategies for established activities. It is not, however, a substitute for the substantive requirement of lawfulness which the controller has primary responsibility to demonstrate compliance with.¹ A risk assessment cannot retroactively validate a processing activity that fundamentally lacks a valid legal basis or fails to



Jalmari Männistö

satisfy core statutory obligations, such as proportionality and data minimization.² The ongoing gauging of proportionality – established in cases such as Digital Rights Ireland and Schrems II – underscores a positive obligation to uphold fundamental rights. This demonstrates that when norms conflict, the necessity and proportionality test acts as a constitutional filter that cannot be bypassed by a controller's internal risk management processes.³ As

1 European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (2018 edn, Publications Office of the European Union 2018); Raphaël Gellert, ‘Understanding the notion of risk in the General Data Protection Regulation’ (2018) 34 *Computer Law & Security Review* 279; see e.g. Case C-60/22, *UZ v. Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), para. 53

2 Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020); Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679* (17/EN WP 248 rev.01, 2017).

3 Brkan M, ‘The essence of the fundamental rights to privacy and data protection: Finding the way through the maze of the CJEU’s constitutional reasoning’ (2019) 20 *German Law Journal* 864

lawfulness itself concerns the choice of the most correct legal basis for the chosen activity, the question increasingly concerns the specific limits found in the wording of these legal bases.

” In practice, this conflict assessment is generally baked into the more clear-cut application of data protection regulation, but the broader statutes require an additional balancing exercise.

The primary avenues for accommodating commercial interests appear to lie in determining processing necessity under contract (Article 6(1)(b) GDPR) – where central questions relate to which contractual obligations are strictly necessary for the performance of a contract which the data subject has willingly entered into⁴ – and legitimate interest (Article 6(1)(f) GDPR) – where the inquiry focuses on which commercial interests are balanced against and do not override fundamental rights.⁵ Whilst legitimate interest has received some love in jurisprudence via recognising commercial interests as simply existing,

the fundamental open question underpinning Art. 6(1)(b) on what obligations and processing are deemed “necessary” under GDPR framework, or *what kind of contracts and related processing would be infringing as-is* is an evergreen topic.

The relevance of supervisory authority guidance done by the European Data Protection Board (EDPB) is integral to the application of data protection regulatory standard to commercial practices. Recently the EDPB has taken a proactive stance in issuing guidelines on edge-cases where there is not as established jurisprudence⁶ – this should be considered as a major theme in the two case studies discussed below especially as EDPB does not merely offer soft law documents but binding guidelines to supervisory authority enforcement.

Recent Finnish cases on data protection and commercial freedom

Case study 1: Verkkokauppa.com Background

Verkkokauppa.com (aptly translating to “onlineshop.com”) is a prominent Finnish e-commerce and retail company listed on Nasdaq Helsinki. Operating a major online retail store alongside physical store locations in Finland the company focuses on consumer electronics, home appliances and related services.

The Finnish Data Protection Ombudsman (“SA”) initiated an inquiry on April 13, 2021, following a complaint regarding a mandatory requirement to register a user account on the company’s portal in order to complete a one-off purchase – preventing the complainant, who declined to register, from making a purchase. The inquiry encom-

passed two main issues: first, the mandatory registration requirement for all online purchases, and second, the practice of retaining customer data “for as long as necessary.”

To the company, these two issues were interlinked: it had made a deliberate commercial decision to adopt an online sales model requiring user account registration, under which personal data was retained for the duration of the underlying customer contract that was in force for the time being and in practice until the customer requested account deletion. In its submissions to the SA, the company stated that the purpose of maintaining continuous user accounts was to provide customers with historical purchase records, warranty tracking, and ongoing service support. The company argued that under the freedom to conduct a business, it had the right to offer a bundled service package requiring user registration to fulfill the contract’s purpose, asserting that “*data protection regulation does not explicitly or implicitly require an undertaking to offer potential customers the option to purchase from an online store without registration*”.

The SA decision

On March 6, 2024, the Data Protection Ombudsman’s Sanctions Board (Tietosuojavaltuutetun seuraamuskollegio) issued decision TSV/26/2020⁷, issuing a formal reprimand under Article 58(2)(b) GDPR and imposing an administrative fine of €856,000 on Verkkokauppa.com Oyj. Additionally, under Article 58(2)(d) GDPR, the supervisory authority issued an order mandating the company to bring its data processing operations into compliance with data protection laws. Specifically, Verkkokaup-

4 *Meta Platforms Inc and Others v Bundeskartellamt* (C-252/21) EU:C:2023:537; Irish Data Protection Commission, decision of 31 December 2022 on Meta Platforms Ireland Ltd’s Facebook service, as affirmed by EDPB, Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)

5 *Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens* (C-621/22), judgment of 4 October 2024, confirming that a purely commercial interest is not categorically excluded from being a legitimate interest under art. 6(1)(f) GDPR.

6 EDPB, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms (adopted 17 April 2024)

7 tietosuojavaltuutettu (Finland), Decision TSV/26/2020 (6 March 2024) <<https://www.finlex.fi/fi/viranomaiset/tietosuojavaltuutettu/2024/2163>>>

pa.com was ordered to define a compliant retention period for customer personal data, cease its practice of requiring mandatory account creation for one-off online purchases, and delete or anonymize all personal data older than the defined retention period without undue delay.

The Data Protection Ombudsman (“SA”) decision involves two primary legal issues, both touching upon the company’s defense based on the freedom to conduct a business:

First, the SA outlines that the case concerns the legality of personal data retention as a whole, which it combines with the commercial choice of having a persistent user account and contract upon. Throughout the decision SA argumentation (and final decision on fines) heavily relies on general principle of storage limitation and the fact that in practice this commercial choice could result in retention period of decades.⁸ The conclusion of a breach is essentially derived from the point that the company had not in fact (due to choice of contracts valid under further notice) determined a storage period (which then could not have been informed). This argumentation is easy to swallow as relying on the primacy of Article 5(1)(e) GDPR (storage limitation) but still essentially establishing that while Article 6(1)(b) GDPR contract processing can be lawful - its proportionality assessment is essentially done on assessing the processing against ultimate fulfillment of Article 5 GDPR general principles.

Second, and more interestingly, the SA assessed the legality (i.e. correct applicability of Art. 6(1)(b)

GDPR) of requiring users to register for one-off online purchases at length as separate from retention time issue.⁹ In its assessment, SA outlined that “*the personal data processing was done in the interest of business*” and “*the main object of the contract could be done without personal data processing*”.¹⁰ The SA’s analysis then relied on an analysis¹¹ of the company’s disclaimed purpose (fulfillment of online purchase) against its assessment of what was possible and necessary for that purpose.

This is a challenging interpretation as the SA relied on the standard of “objectively necessary”, as flowing from EDPB dispute mechanism decision,¹² and standard-setting Bundeskartellamt CJEU-decision¹³ which set out a strict fundamentality test on Art. 6(1)(b) GDPR which was used to distinguish targeted advertising as not belonging to the scope of social media’s contract legal basis (and as provided by unrelated third parties). However in this case, the argumentation leads to a point where not just a partial commercial activity but the whole framework of requiring registration would be prohibited as being *possible* to conduct in a more limited manner, and thus not fulfilling the legality requirement of Arti-

cle 5(1)(a) GDPR. The SA decision underlines the issues concerning application of this objective necessity standard as

- a. the objectivity can essentially disregard the original intention and goal sought by the company in establishing a service containing multiple different processing activities; and
- b. result in the wholesale infringement of the processing if one of these processing activities can be distinguished as not strictly necessary for a narrow goal of the contract.

Following strictly *this* interpretation of objective necessity – as one without necessarily taking into account the service as a whole under Article 6(1)(b) GDPR assessment - the use of contract-based data processing would essentially need to identify the simplest form of service performance (for which there is no explicit legal standard for determination) and compare each personal data processing against that purpose.

Administrative court decisions and final analysis

As typical of GDPR fines of sufficient size, the company appealed the decision to the administrative court. The administrative court decision¹⁴ (Dnro 2096/03.04.04.04.01/2024) is rather uneventful¹⁵ in its content and basically repeats assessment in the SA decision focusing on the issue with data minimisation and retention

⁸ relying on e.g. European Data Protection Board (EDPB), ‘Guidelines 4/2019 on Article 25 Data Protection by Design and by Default’ (Version 2.0, adopted 20 October 2020).

⁹

¹⁰ Paras 64-65 of the decision

¹¹ See, for example, the justification provided in European Data Protection Board (EDPB), ‘Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects’ (Version 2.0, adopted 8 October 2019).

¹² European Data Protection Board (EDPB), ‘Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)’ (adopted 5 December 2022).

¹³ Case C-252/21 *Meta Platforms Inc. and Others v Bundeskartellamt* ECLI:EU:C:2023:537.

¹⁴ Helsingin hallinto-oikeus (Helsinki administrative court) Decision 2096/03.04.04.04.01/2024

¹⁵ There is a salient procedural question for another text of at which part of the SA consultancy becomes and infringement procedure requiring sufficient hearings, and before which the company should be given possibility to rectify its infringement.

times – and upholding the fine while lowering its amount (792 639 EUR). While the SA decision (or the attached sanctions board decision) does not clearly distinguish whether the fine is issued on the basis of merely infringement of minimisation and retention times as resulting from commercial decision to require registration, or as that mandatory registration forming a partial basis of infringement independently, the administrative court’s decision streamlines this by assessing the fine’s validity and amount solely on the context of retention times (as a result of commercial decision). The distinction is quite material as then the administrative court, nor the supreme administrative court in the following appeal¹⁶, did not assess the legality of mandatory registrations *an sich* similarly as in the SA decision. On the contrary, both the administrative court and supreme administrative court separately stated that the SA decision should not be interpreted as ruling mandatory registration as unlawful, but rather only on its resulting data retention.¹⁷ While I somewhat disagree on this assess-



Illustrasjon: Coulorbox

ment of the SA decision¹⁸ this assessment results in an interesting what-if:

1. As the only issue by which the courts upheld the fine concerned the failure to establish and communicate retention times¹⁹ – this assumes that the issue of mandatory registrations and its legal basis did not act as a basis of the fine;
2. Then the interesting question is whether the fine would have been upheld (or even issued at all) if the retention time infringement had been lesser or non-existent. In other words, it seems that the company could justify its mandatory registration with freedom of commerce.

Contrary to this recognition, the SA position against mandatory registrations has also been since enshrined in the EDPB Recommendation 2/2025 where it is still maintained

18 Paras 62-67 clearly outline the argument for missing legal basis of mandatory requirements - same sentiment which the EDPB reiterated in its following guidance Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites

19 Also important to note that the administrative court lessened the amount of the fine following the company’s efforts to already rectify the infringement

that “*necessity test required [...] is unlikely to be met*”.

Scenario 2: Posti (OmaPosti)

Background

In many ways similar to the [Verkkokauppa.com](#) case discussed above, another case concerning freedom of commerce defence concerns online services and its necessity test. Continuing on the theme of aptly named companies and services, Finnish postal company Posti Jakelu Oy was issued a €2.4 million fine for their “OmaPosti-postilaatikko”-service (again aptly named eng: “OwnPost-postbox”) bundling together multiple different online services with registration to just one.²⁰ This OmaPosti-service combines together multiple different online services, such as postal address changes, parcel tracking, rerouting mail and e-post which multiple Finnish authorities use by default. Posti’s service design maintained that in order to use the online services you had to a) register to the service, and b) by default take the service into use in full. Meaning that if you wanted to conduct an address change, this automatically opened up an e-post inbox for you.

On July 7, 2020, the Finnish SA opened an investigation following customer complaints regarding the mandatory activation of the digital inbox. The inquiry addressed two main issues: transparency shortcomings during account onboarding, and the mandatory bundling of all OmaPosti service features upon registration. The fine imposed by the SA was based specifically on the mandatory service bundling, while the transparency failures received a formal reprimand.

SA decision

Similarly to the case in [Verkkokauppa.com](#) above, Posti claimed

16 *Korkein hallinto-oikeus* (Supreme Administrative Court of Finland), Decision KHO 2026/1604

17 KHO 12.6.2026/1604 para 10 “According to the Administrative Court’s decision, it does not appear from the Data Protection Ombudsman’s decision that the company’s practice – requiring customer registration to make a single purchase in the online store – was considered in itself to be in violation of the General Data Protection Regulation or other data protection regulations. Therefore, the Administrative Court has assessed the legality of the company’s practice only insofar as whether it has resulted in an unlawful situation regarding the retention period of personal data.”

20 Tietosuojavaltuutettu (Finland), Decision of 13 November 2024 (Finlex 2024/2363).

throughout the consultancy that it had the right under freedom of commerce to design its service offering how it sees fit and combine different functionalities in its service as one unified service and offer that by default to all its users without possibility to opt-out of single functionalities. Similarly to Verkkokauppa.com Posti argued that applicable data protection regulation lacks general principles which would determine which specific parts of a service are allowed to function under the same legal basis and which would need to be distinguished - and thus neither the SA would have the authority to determine this.

The SA relied generally on the exact same legal sources and argumentation²¹ as in the case concerning Verkkokauppa.com (concerning legal basis of mandatory registration) and maintained that specifically the e-post inbox (OmaPosti-postilaatikko) *can* be separated from the performance of post rerouting and cannot thus be considered objectively necessary for the performance of contract which the user might seek by entering into a contract. The personal data processing related to e-post inbox was then outside of the contractual legal basis and its data processing unlawful.

Due to Posti relying multiple times on freedom of commerce defence, the SA addressed this shortly stating that the decision is not about the evaluation of a specific business practice, or a part of a service, but rather on whether a data controller has a valid legal basis for its processing. A legal chicken-and-egg.

Administrative court decision and final analysis

Following Posti's appeal of the SA decision, on 3 November 2025, the Helsinki administrative court gave a shock decision on the matter – the €2.4 million fine was overturned in its entirety.²² The court's decision addressed both streams of inquiry and validated the first concerning lack of sufficient information to the inbound users of the OmaPosti-service – however the fine was solely based on the invalidity of Posti's contractual legal basis in which the court disagreed with the SA.

In a well argued decision the court compared the Posti-processing with the processing and standard set out in Bundeskartellamt-decision: whereas the personalisation of marketing content on a social media platform cannot be justified as necessary or otherwise “important” to the processing which the underlying contract concerns (even if it would be “useful” for the user) because the user can be offered the same service in an equivalent manner without that processing and importantly without sharing the personal data to third parties for this purpose. The court recognised that the situation with Posti differs from Meta's advertising personalisation in a material manner as OmaPosti was solely Posti's own service and the processing was result of its own commercial choices and not that of third parties. In reference to EDPB Guidelines 2/2019 the court recognised that OmaPosti-service had internal service justifications to bundling the services together instead of solely the company's ancillary commercial gain or resulting in additional personal data processing unnecessary for that service-purpose. Bundling the e-post inbox to the other services was justified in

the same legal basis and contractual freedom - the fine was overturned.²³

From an immediate viewpoint it might seem that the [Verkkokauppa.com](https://www.verkkokauppa.com) and Posti -cases might have very different building blocks as one fine maintained and the other overturned, but when we disregard Posti's information obligation failures and [Verkkokauppa.com](https://www.verkkokauppa.com)'s lack of retention times, the cases have very similar grounding. In both cases the company acted on the basis of Article 6(1)(b) GDPR, bundling multiple service functionalities together, and were challenged on the necessity of some of those functionalities. In both cases the administrative courts confirmed (against the SA) that the controller had the commercial freedom to determine the scope of their data processing on contractual basis (provided that the functionality was necessary).

From this point of view, it would seem that the objectivity and necessity standard set out in Bundeskartellamt and relevant EDPB guidelines gives more leeway to commercial actors to offer service packages on the objective they have contractually defined, as long as the parties to the processing are the same and it contributes to the service's functionality instead of just independent commercial interest.

In conclusion:

Jurisprudence addressing the intersection of contractual necessity and commercial discretion under the GDPR continues to evolve. Recent judicial decisions in Finland indicate a balanced approach that protects consumer data rights while respecting controllers' constitutional freedom to conduct a business.

Jalmari Männistö, Secretary of Finnish IT-law association (IT-oikeuden Yhdistys ry), Legal counsel (technology & contracting) - Epassi Group.

²¹ To be clear the SA employed a more deep analysis of CJEU case C-252/21 para 98 wherein it relied on the controller's obligation to be able to show why each processing is necessary for the main purpose of the contract.

²² Helsingin hallinto-oikeus (Helsinki administrative court) 2096/03.04.04.04.01/2024

²³ For clarity, the matter is still pending on the Finnish Supreme Administrative Court