IRDG Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU Faculty of Law

UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES No. 23-03

THE DATA ACT PROPOSAL

Literature Review and Critical Analysis

Moritz Hennemann / Benedikt Karsten / Marie Wienroeder / Gregor Lienemann / Gordian Ebner (Eds.)

Part III (Art. 23-34, 36-42)

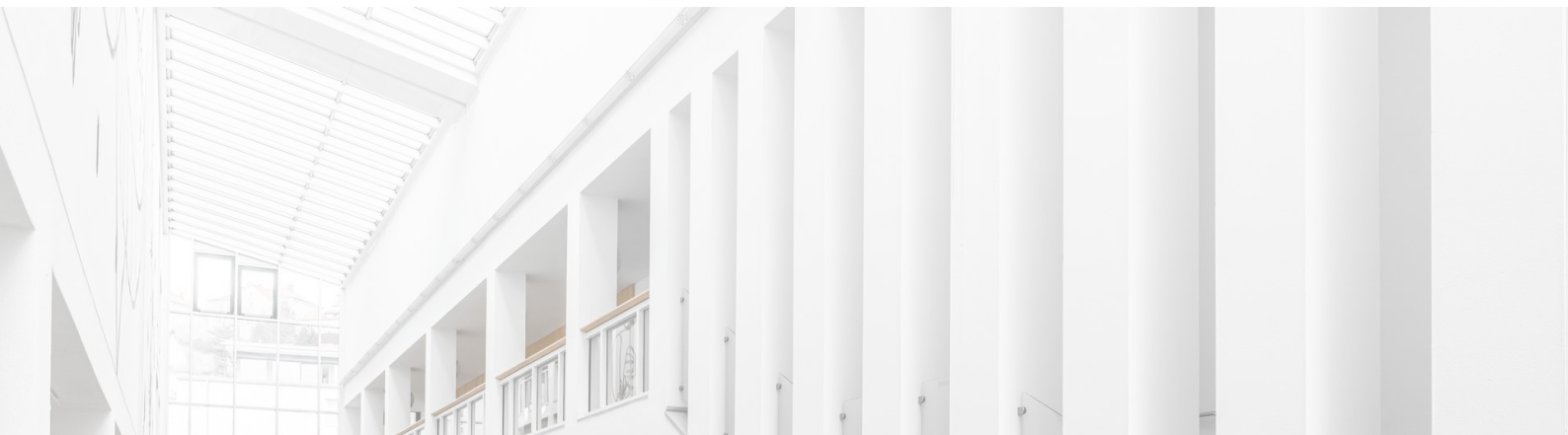
Chapter VI: Switching Between Data Processing Services
Chapter VII: International Contexts Non-Personal Data Safeguards
Chapter VIII: Interoperability
Chapter IX: Implementation and Enforcement
Chapter XI: Final Provisions

by

Gregor Lienemann / Marie Wienroeder

Version 1.0

January 2023



Place of Publication

University of Passau IRDG
Innstraße 39
94032 Passau
https://www.jura.uni-passau.de/irdg/

Editors and Authors

Moritz Hennemann is a Full University Professor, holding the Chair of European and International Information Law, University of Passau Law Faculty since 2020. His research focuses on private law, business law, data law, media law, and information law, including from a comparative perspective. He holds degrees in law from the Universities of Heidelberg (2009), Oxford (M.Jur., 2011), and Freiburg (Dr. jur., 2011). He was a postdoctoral researcher at the University of Freiburg (Habilitation, 2019), a visiting researcher at Harvard Law School and an affiliate to the Berkman Klein Center for Internet & Society, Harvard Law School.

Benedikt Karsten is an academic research assistant and doctoral candidate in law at the Chair of European and International Information Law, University of Passau Law Faculty since 2022. His research focuses on data law. He holds a degree in law from the University of Passau (2020) and is a fully qualified lawyer (Ass. jur., 2022).

Marie Wienroeder is an academic research assistant and doctoral candidate in law at the Chair of European and International Information Law, University of Passau Law Faculty since 2022. Her research focuses on data law. She holds a degree in law from the University of Passau (2022).

Gregor Lienemann is an academic research assistant and doctoral candidate in law at the Chair of European and International Information Law, University of Passau Law Faculty since 2021. His research focuses on data portability and on the intersection of data protection and competition law, including from a comparative perspective. He holds degrees in law from the Universities of Munich (2020) and Reading (LL.M., 2021).

Gordian Ebner is an academic research assistant at the Chair of European and International Information Law, University of Passau Law Faculty since 2020. His research focuses on data protection law, especially data-related information duties. He holds degrees in law from the University of Passau (2020 and Dr. jur., 2022).

https://www.jura.uni-passau.de/hennemann/

Abstract

This three-part publication critically evaluates the Commission's Proposal for a Data Act. It provides an in-depth analysis of the Proposal. The concept of the Act is critically examined and the instruments proposed are thoroughly evaluated and put into context. The existing literature

on the Act is mapped and mirrored. Proposals for amendments to the Act are considered. This publication aims to contribute to the on-going debate about and the legislative process of the Act.

Cite as

Lienemann, G. / Wienroeder, M. (2023). Part III (Art. 23-34, 36-42), in: Hennemann, M. / Karsten, B. / Wienroeder, M. / Lienemann, G. / Ebner, G. (Eds.). The Data Act Proposal – Literature Review and Critical Analysis. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 23-03.*

All parts of this three-part publication on the Data Act Proposal are available at https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/.

Keywords

Data Act, Data Governance, EU, Data Strategy, Cloud Services, Non-Personal Data Transfers, Interoperability, Data Portability

Foreword by the Editors

Dear Fellow Reader,

Since February 2022, the wider public and the Data Law community in particular has had the chance to have a look at the Commission's Proposal for a Data Act. From then on, manifold discussions have begun – including within the European Parliament. Up to this date, we have seen three proposals by the Council's presidency to amend the Commission's proposal – and at least one more is said to come. To assist this process, we have – as a first step – published a Data Act – Article-by-Article Synopsis (systemizing provisions, recitals, and definitions) in March 2022.

This Literature Review and Critical Analysis of the Data Act Proposal – as a second step – provides an (more) in-depth analysis of the Proposal. It is presented in three parts / documents (all accessible here) and also builds upon first contributions to the debate by Hennemann, M. / Steinrötter, B., Data Act – Fundament des neuen EU-Datenwirtschaftsrecht?, *Neue Juristische Wochenschrift (NJW)* 2022 (21), 1481-1486 and Ebner, G., Information Overload 2.0? – Die Informationspflichten gemäß Art. 3 Abs. 2 Data Act-Entwurf, *Zeitschrift für Datenschutz (ZD)* 2022 (7), 364-369; Karsten, B. / Wienroeder, M., Der Entwurf des Data Act – Auswirkungen auf die Automobilindustrie, *Recht Automobil Wirtschaft (RAW)* 2022, 99-105; Hennemann, M., Datenrealpolitik – Datenökosysteme, Datenrecht, Datendiplomatie (2022) *University of Passau IRDG Research Paper Series No. 22-18*).

The concept of the Data Act is critically examined and the instruments proposed are evaluated and put into context. Especially, the study also considers the on-going legislative debate within the European Parliament and with regard to the amendment proposals of the Council Presidency. In addition, reference is not only given to the growing literature on the Data Act proposal (there is very much…), but the current state of discussions is mapped and mirrored – and, where appropriate – this Literature Review and Critical Analysis takes a stand on existing proposals for amendments to the Act and / or proposes further amendments to be considered.

We have especially looked at those parts of the Act (especially Chapter VI on "Switching between Data Processing Services") which have not got the same attention than the omnipresent access rules of Art. 4 et seq. Part I includes an Executive Summary.

This Literature Review and Critical Analysis will be amended in due course – it is *work-in-progress* and just an Open Access-Version 1.0 – and is meant to be published in a revised version after the finalisation of the Data Act (whenever that might be…).

We are more than happy to hear your thoughts about this Literature Review and Critical Analysis in general and about what we have missed – and warmly welcome recommendations in order to close gaps and to correct us! Please drop us an e-mail to moritz.hennemann@uni-passau.de.

We like to thank the entire team at the chair of European and International Information and Data Law and at the Research Centre for Law and Digitalisation (FREDI) for their extremely valuable support in the drafting process and for taking the burden of formatting the documents.

Sincerely yours,
Moritz Hennemann, Benedikt Karsten, Marie Wienroeder,
Gregor Lienemann & Gordian Ebner

Contents

VIII. Switching between Data Processing Services (Art. 23-26)

Chapter VI ('Switching Between Data Processing Services', Art. 23-26) introduces minimum regulatory requirements of contractual, commercial, and technical nature, imposed on providers of cloud, edge and other data processing services, to enable switching between such services. Where technically feasible, a minimum level of functionality for customers shall be preserved after switching to the new service.[1]

The Commission's Rationale for Taking Regulatory Action

In its Impact Assessment Report, the Commission observes the trend of integrated cloud ecosystems combining a variety of services from which customers are in effect prevented to extricate themselves due to contractual, economic, and technical switching costs.[2] As the value of a given cloud service is typically contingent upon the scale of its customer base, network effects towards cloud environments to manage large one-stop shops have occurred.[3] Self-regulatory approaches, most notably the SWIPO Codes of Conduct developed in accordance with Art. 6 Regulation (EU) 2018/1807, have so far been unused save for a few providers[4] and have thus proven insufficient to address this so-called 'vendor lock-in' (cf. Rec. 70). As a result, the Commission regards the requirements under Chapter VI as a more potent policy option to lower market entry barriers for data processing services (Rec. 69) and thereby achieve an innovative and "seamless multi-vendor cloud environment" (Rec. 76).

The Notion of Data Processing Services (Colliding with Other Actors of the Digital Economy)

Despite no such link having been established within the Proposal, the access and portability regime for IoT-related data devised in Chapter II should be an immediate consideration in the context of switching from one data processing service to another. Datasets stemming from the use of IoT devices will often be fed into a cloud-mediated system on which they are stored remotely.[5] What is more, providers of IoT services are increasingly relying on so-called edge computing, processing data more locally to achieve quicker response times from sensors and mitigate privacy concerns.[6]

"[L]imited possibilities for the portability of data generated by products connected to the Internet of Things" (Rec. 19) are bound to persist if they cannot be easily unlocked from the existing and migrated to a new cloud environment by way of switching. [7] Among the purposes for introducing the bulk of Chapter VI obligations, rendering operational the rights conferred to data users under Chapter II should be highlighted. At present, this nexus of IoT and cloud (regulatory) ecosystems can only be inferred and is complicated by the fact that edge computing

---

[1] Commission, COM(2022) 68 final Explanatory Memorandum, p. 16.

[2] Commission, 'Impact Assessment Report Accompanying the document Proposal for a […] Data Act', SWD(2022) 34 final, pp. 19 et seq.

[3] Schnurr, D., Switching and Interoperability Between Data Processing Services in the Proposed Data Act, 2022, p. 8.

[4] Id., p. 20; cf. https://swipo.eu.

[5] Cf. vbw, Data Act – Anpassungsbedarf aus Sicht der Bayerischen Wirtschaft, 2022, p. 16 (noting more generally that data holders and recipients will frequently rely on cloud solutions).

[6] Hon, W.K. et al., 'Cloud Technology and Services' in: Millard, C. (ed.), *Cloud Computing Law* (OUP, 2nd edn 2021), p. 17.

[7] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 60 n. 164.

services – probably by mistake – merely appear in some of the Recitals, but do not unequivocally form part of the definition of data processing services in No. 12 of Art. 2.[8]

While said definition is extensive in most regards[9], it exempts online content services under Art. 2(5) Portability Regulation (EU) 2017/1128 (of which music and video streaming services might form the most prominent sub-set) from having to comply with the obligations introduced by Chapter VI. No reason is provided for the omission, nor can it be justified by the absence of lock-in scenarios when using these services.[10] *Geiregat* surmises that the Commission wrongly took Regulation 2017/1128 to cover the issue of switching, when in fact it deals with cross-border availability of online content services between member states ("geo-portability").[11] The exclusion of online content services could also be explained by the fact that audio-visual media (on streaming platforms) are usually controlled by third-party copyright[12], the protection of which could be valued so high as to override *ex-ante* potentially infringing switching operations departing from such platforms. However, this outcome could likewise be achieved by the simple clarification that audio-visual media broadcast by online content services should not be considered digital assets (cf. Rec. 72).[13] At the very least, the Commission should lay out (e.g., in Rec. 71) why providers of online content services are exempt from Chapter VI obligations.

It has been submitted from a comparison with the somewhat co-extensive obligations imposed on gatekeepers under the Digital Markets Act – which has recently been adopted as Regulation (EU) 2022/1925 – that the requirements in Chapter VI to facilitate switching would significantly raise market entry barriers for small and medium-sized enterprises (SMEs).[14] In a broadly similar vein, the IMCO Draft Opinion advocates for exempting cloud services that have been custom-built or which operate on a trial basis.[15] We concur that an exception be added for SMEs to the extent that the mandatory contractual terms under Art. 24(1) can be wholly or partially waived on the grounds of technical unfeasibility.

On a terminological matter, the IMCO Draft Opinion rightly suggests replacing the concept of "data processing service" with "cloud computing service", which has achieved the status of a well-recognised definition, both by standardisation bodies and in Union legislation.[16] Naturally, the terminological shift to cloud computing services should not factor out edge computing services which, as just pointed out, deserve mention in the definition under No. 12 of Art. 2.

---

[8] See on the one hand, Rec. 69 and Rec. 71, Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 61 n. 169.

[9] See above on Art. 2(12).

[10] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 62 para. 170.

[11] Geiregat, S., 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, p. 30 et seq. at para. 31.

[12] Cf. Rec. 62 of Directive (EU) 2019/790; relatedly, Geiregat, S., 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, p. 38 et seq. at para. 40 (on the unclear interface with IP rights).

[13] See below on Art. 23; similarly, Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 63 n. 171.

[14] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 112 et seq.

[15] IMCO PE736.701, p. 46.

[16] IMCO PE736.701, pp. 23 et seq.

Chapter VI – Basis for a Dedicated 'Cloud Portability Right'?

The obligations to remove obstacles to the porting of data, applications and other digital assets (Art. 23(1)(c)) are targeted at the data processing services just outlined. Whether and how these obligations translate to a distinct right that customers may invoke against providers in broadly the same way as the right granted in Art. 5(1) is up to debate – and should be kept separate from the question if a new portability right in the cloud sector is necessary as well as conducive to the current framework under European Union law.

Geiregat extrapolates from Art. 23(1)(c), jointly read with Art. 24(1) and Art. 26, the creation of a statutory, i.e. "self-standing, immediately enforceable subjective right"[17]. The MPIIC proceeds on the assumption of a contractual right that entails both switching and portability obligations.[18] Relatedly, the Weizenbaum Institute derives from Art. 24(1) a right to switch between providers, along with the conditions for exercising that right.[19] The members of CiTiP take a similar view, interpreting Art. 23(1) in the sense of a "positive obligation to deliver on switching", which the Commission failed to frame as an explicit right to switch.[20]

In our opinion, caution is merited on what the obligations presupposed in Art. 23(1)(c) and carved out in greater detail in Art. 24(1) and Art. 26 truly amount to and whether *Geiregat*'s hypothesis of a self-standing, distinct "cloud portability right"[21] holds up to scrutiny. Importantly, Art. 24(1) does not emulate the language of Art. 5(1), which is generally understood as a right to port IoT-related data bearing some resemblance to Art. 20(2) GDPR.[22] Instead, it prescribes a contractual framework for the "rights (…) in relation to switching". To fully grasp the ramifications of this subtle yet crucial difference in semantics (plural instead of singular), Art. 24(1) has to be related back to the overarching mandate under Art. 23(1)(c) to remove all obstacles to porting – contractually, technically or otherwise. Accordingly, the originating provider mainly has a *negative obligation* to refrain from obstructing the switching process, on top of which they are bound by a *positive obligation* to assist (in) the switching process under Art. 24(1)(a).

The first-mentioned obligation, surfacing in Art. 23(1)(c), lays the ground for uninhibited porting to take place and, from the perspective of the consumer, could be labelled as a "right to switchability".[23] Critically, this was also how the Commission designated the policy option in its Impact Assessment Report which prevailed over keeping the self-regulatory framework of Regulation (EU) 2018/1807.[24]

---

[17] Geiregat, S., 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, p. 40 at para. 43. Cf. also id., p. 29 at para. 28.

[18] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 61 n. 167.

[19] Weizenbaum Institute for the Networked Society, Position Paper regarding Data Act, 2022, p. 24.

[20] Ducuing, C. / Margoni, T. / Schirru, L. (Ed.), *CiTiP Working Paper* 2022, 60.

[21] Geiregat, S., 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, p. 29 at para. 28 and *passim.*

[22] Commission, 'Impact Assessment Report Accompanying the document Proposal for a […] Data Act', SWD(2022) 34 final, p. 67; cf. Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 27 n. 69 and *passim*; Ducuing, C. / Margoni, T. / Schirru, L. (Ed.), *CiTiP Working Paper* 2022, 28.

[23] Commission, COM(2022) 68 final Explanatory Memorandum, p. 11.

[24] Commission, 'Impact Assessment Report Accompanying the document Proposal for a […] Data Act', SWD(2022) 34 final, p. 37.

The subsequent obligation, i.e. to assist with the switching process (what brings to mind a *Mitwirkungspflicht* under German legal terminology), should technically be regarded as a right to receive migration support[25] or, economically, as mandatory 'exit management'. Of course, Art. 24(1)(a)(1) also establishes a heightened duty (see also, the opening sentence of Rec. 72) to *complete* the switching process[26] provided that this is technically feasible. Owing such a completion of the switching process would indeed mean a right to have the digital assets in question ported directly to the infrastructure of the destination service. However, the *caveat* of technical feasibility is likely to be a salient (and therefore less than exceptional) ground for circumventing this right[27] in the absence of operational standards under Chapter VIII. The experience with the same *caveat* in Art. 20(2) GDPR foreshadows limited efficacy and at least some level of under-enforcement.[28] From the incoherent use of the term porting (especially in relation to on-premise systems[29], one may narrow down the practical scope of this right even further in favour of *in-situ* access where interoperability is less of an issue.

Consistent with the plural form used in Art. 24(1) ("rights"), Chapter VI then does not give rise to a directly enforceable cloud portability right, but to a bundle of three interconnected entitlements by virtue of the contract between the customer and the provider of the originating service:

(1) the right to demand a position at the originating service free from obstacles to 'switchability'

(2) the right to have the provider of the originating service assist with the switching process

(3) the right to have ported the digital assets at issue to an on-premise system or (possibly) directly to the infrastructure of the destination service.

What these rights have in common is their origin within the contract. The concern that the originating service provider may conceivably take advantage of their bargaining position and alter its contents in a manner contrary to Art. 24(1) should therefore not be neglected.[30] For this provision specifically, relying solely on public enforcement by the competent authority under Art. 31(2)(c) falls short in remediating the switching-related obstacles faced by customers.[31]

---

[25] For the situation under prior law, cf. Schuster, F. / Hunzinger, S., *CR* 2015, 277 (278 et seq.).

[26] Council Presidency 2022/0047(COD) – 13342/22, p. 57 erroneously moves to replaces this expression with "porting process".

[27] Geiregat, S., 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, p. 36 at para. 37.

[28] On a similar prospect for the Chapter II portability right, cf. Leistner and Antoine, p. IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 113 et seq.

[29] See below p. 10.

[30] Geiregat, S., 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, p. 40 at para. 42.

[31] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 67 n. 182.

We concur with calls for effective private enforcement in the court system, assessing the conformity of the contract with the requirements of Art. 23 et seq.[32]

Functional Equivalence – A Feasible Concept?

As previously discussed[33], the Proposal eschews specifying the core elements of a given service for which functional equivalence must be ensured by the originating provider.

Unless these are sufficiently narrowed down, ensuring the same output on core elements of the service after switching would likely require the originating service provider to have some form of access to the infrastructure of the destination provider, thus potentially compromising trade secrets. It is for this reason that the IMCO Draft Opinion has moved to discard the concept of functional equivalence altogether.[34] Conversely, *Leistner* and *Antoine*, writing in an advisory capacity to the Committee on Legal Affairs (JURI), regard functional equivalence as "practically central" *en route* to interoperable ecosystems and IT infrastructures between the originating service and the destination service, with some disagreement on the details of the corresponding obligation.[35] In its 2nd compromise text, the Council Presidency develops a kind of *media sententia* and suggests reigning in the overly ambitious notion of functional equivalence in a redrafted part of Rec. 72 along the following lines:

> "Services can only be expected to facilitate functional equivalence for the functionalities that both the originating and destination services offer. This Regulation does not instate an obligation of facilitating functional equivalence for data processing services of the PaaS and/or SaaS service delivery model."[36]

On the first point, the Council Presidency has correctly identified the – far from unlikely – scenario that the originating service possesses functionalities which are absent from the destination service (take certain applications and channels for team collaboration within an elaborate SaaS environment or, more generally, unused features *prior* to switching). The second point is a favourable distinction among the wealth of cloud services of varying complexity, but is perhaps better suited to clarify Art. 26(1) not applying to PaaS and SaaS cloud businesses.[37]

Moreover, the definition of "functional equivalence" in Art. 2(14) is not immune to regulatory friction since it does not consider the interplay with a similar term defined in Art. 2(12) of the Digital Content Directive:

> "'functionality' means the ability of the digital content or digital service to perform its functions having regard to its purpose;"

---

[32] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 67-68 n. 183-184; contra Geiregat, S. 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, p. 40 at para. 43 (criticising this approach as a "detour around national private-law remedies").

[33] See above on Art. 2(14).

[34] IMCO PE736.701, p. 3.

[35] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 113 et seq.; further, see below on Art. 26.

[36] Council Presidency 2022/0047(COD) – 13342/22, p. 29.

[37] See below on Art. 26.

One is naturally drawn to compare both definitions and wonder if the yardstick of functionality has a bearing on "functional equivalence" within the meaning of the Proposal.[38] If answered in the affirmative, specific contractual assurances on what the originating service may perform in terms of output could come into play.[39] While the Proposal cannot be construed to conclusively lean one way or the other on this question, it should be noted that the *removal* of contractual obstacles to the detriment of switching – as the overarching theme to ensuring functional equivalence under Art. 23(1)(d) – would hardly require *preserving* each contractual arrangement on the core elements of the originating service.

Proposed Amendments

Art. 2(12)

– Abandon the unwieldy term "data processing service" in Art. 2(12) in favour of "cloud service" – explicitly referring to edge computing within a definition revised accordingly.[40]

Art. 24

– Add a third paragraph to Art. 24, excluding SMEs from the contractual requirements under paragraph 1 of the same article where they can show technical unfeasibility. The exception should be drafted in a manner akin to Art. 7(1).

Rec. 74

– Insert a new second sentence into Rec. 74: "Services can only be expected to facilitate functional equivalence for the functionalities that both the originating and destination services offer."[41]

Art. 31

– Redraft Art. 31 to reflect the fact that member state courts may review the contractual requirements under Art. 24(1) and order appropriate remedies to the benefit of customers.

1. Removing Obstacles to 'Switchability'(Art. 23)

Art. 23(1) merges the specific means and ends of regulation to ensure that customers can switch to another data processing service (which Rec. 72 labels the 'destination' service). The Council Presidency seeks to introduce a definition for 'customer' in a new No. 12a of Art. 2, thus addressing both consumers and business entities as a

> "a natural or legal person that has entered into a contractual relationship with a provider of data processing services with the objective of using one or more data processing services."[42]

[38] Ducuing, C. / Margoni, T. / Schirru, L. (Ed.), *CiTiP Working Paper* 2022, 63.

[39] Ducuing, C. / Margoni, T. / Schirru, L. (Ed.), *CiTiP Working Paper* 2022, 63.

[40] Geiregat, S. 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, p. 52.

[41] Council Presidency 2022/0047(COD) – 13342/22, p. 29 (advocating for a change to Rec. 76).

[42] Council Presidency 2022/0047(COD) – 14019/22, p. 37; concurringly, Geiregat, S. 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, p. 29 at para. 29.

As to the *means* of switching, providers of data processing services are obliged to implement the measures fleshed out in the subsequent Art. 24-26. Art. 23(2) stresses in this regard that the burden of compliance rests solely with the original provider (i.e. the entity offering the 'originating' service, cf. Rec. 72).

These obligations are related back to four stages or *ends* of a customer-friendly switching process, the associated obstacles to which providers are meant to remove when implementing the measures under Art. 24-26.[43] The first two stages concern private autonomy and more specifically customers' freedom of contract, namely the ability to terminate the original service agreement within (at most) 30 days' notice (Art. 23(1)(a)) and the ability to conclude a new service agreement with the destination service (Art. 23(1(b)). As to the former, the notice period has been criticised for clashing with widely accepted commercial practices, namely with a fixed minimum duration which is distinctive for some contractual arrangements.[44] The Council Presidency suggests that at most, the customer has to give two months' notice, and that the precise notice period should form part of the mandatory contractual terms under Art. 24(1).[45]

The baseline scenario envisioned by the Commission appears to be a one-way process of data migration by the customer from the originating service to the destination service. Upon first blush, a continued use of the originating service (so-called multi-homing) by the customer after transitioning to the destination service would therefore fall outside the purview of switching in this sense due to the termination of the prior contractual arrangement. The opening sentence of Rec. 72 reiterates along these lines that switching

> "[…] encompasses *all* conditions and actions that are necessary for a customer to terminate a contractual agreement of a data processing service, to conclude one or multiple new contracts with different providers of data processing services, to port all its digital assets, including data, to the concerned other providers *and* to continue to use them in the new environment while benefitting from functional equivalence." (emphasis added)

In light of Chapter VI's principal aim to combat vendor lock-in and to increase customers' margin of choice between competing data processing services, one wonders whether such a definitive understanding of the action of switching was actually intended by the Commission. Namely, customers will often choose to engage with more than one platform (e.g. for cloud storage) in order to have multiple access and backup methods with respect to the relevant data stock.[46]

Art. 23(1)(c) stipulates that existing barriers for customers to port data (including meta-data as per Rec. 72), applications, and other digital assets must be removed, thus complementing and preparing the exercise of the right to data portability under Art. 20(1) GDPR in B2C settings where personal data are involved (cf. Art. 1(3)). Even though no mention is made of the right to erasure pursuant to Art. 17 GDPR, it would likely also come into play at this third stage, i.e.

---

[43] The wording at the start of the second sentence of Art. 23(1) ("In particular") does not seem to imply that the measures to be taken by providers would have to go beyond what is prescribed in Art. 24-26.

[44] Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, 2022, p. 14.

[45] Council Presidency 2022/0047(COD) – 14019/22, p. 56: new Art. 24(1)(aa).

[46] Goode, S., Understanding Single Homing and Multihoming User Switching Propensity in Cloud File Hosting Service Relationships (2020) e-Service Journal 34 (42).

once the service agreement with the originating provider has been terminated, upon request by (data subject) customers (cf. Rec. 7 on the interplay with the GDPR).

The peculiar choice of the umbrella term 'digital assets' – a term that has hitherto largely been endemic to debates on so-called 'digital inheritance'[47] – demonstrates that the notion of data under Art. 2(1) translates to a semantic, not a syntactic representation of information. Adding a new No. 12b to Art. 2, the Council Presidency now defines 'digital assets' as "elements in digital format for which the customer has the right to use, independently from the contractual relationship of the data processing service it intends to switch away from […]".[48] Some confusion remaining over the meaning of 'applications' as part of the overarching concept of 'digital assets' should be addressed. As it stands, the term could be misconstrued to cover the whole service offering of the originating provider to the customer.[49] To avoid ambiguity, 'applications' should be framed in terms of IT architecture, for instance as computer programs that the customer could use on the originating provider's cloud infrastructure.[50]

Lastly, Art. 23(1)(d) highlights functional equivalence in the use of destination services covering the same service type as the final stage of the switching process and anticipates the requirements to be observed under Art. 26. In line with the general dismissal of the idea of functional equivalence as unrealistic[51], the associated obligation should not stand in the opinion of the IMCO Draft Opinion.[52]

Proposed Amendments:

- Clarify position (e.g., in Rec. 69) regarding multi-homing beyond the transition period – does termination of the prior service agreement constitute a necessary prerequisite for "switching" and for holding applicable Art. 24-26?

Rec. 72

- Redraft Rec. 72 to read that porting to the destination service entails, *vice versa*, deletion of personal data pursuant to Art. 17 GDPR where the customer is a data subject.
- Relocate the definition of digital assets in Rec. 72 to a new number under Art. 2, adding a sentence that audio-visual media broadcast by online content services pursuant to Art. 2(5) of Regulation (EU) 2017/1128 should not be considered digital assets.
- Repurpose Rec. 72 with a definition of "applications" that highlights them as pieces of IT infrastructure (i.e., computer programs) used by the customer on the originating service.

[47] Geiregat, S. 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, p. 33 at para. 33 with further references.

[48] Council Presidency 2022/0047(COD) – 14019/22, p. 37.

[49] Bitkom, 'Bitkom Position Paper EU Data Act Proposal' (19 April 2022), 2022, p. 10.

[50] Geiregat, S. 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, p. 32 at para. 33.

[51] See above p. 5.

[52] IMCO PE 736.701, p. 35.

2. Contractual Enablers of Switching (Art. 24)

Whereas Art. 23 requires *ex negativo* that providers of data processing services do away with certain obstacles to 'switchability', Art. 24 stipulates the minimum content (rights and corresponding obligations) arising from the contractual agreement between customer and originating provider when it comes to switching to a new (destination) service. In certain instances, originating services will in fact have to observe the customer's rights under one service agreement while holding the same corresponding rights under a different service agreement with another (upstream) data processing service. Rec. 73 acknowledges this likely dual role:

> "Where providers of data processing services are in turn customers of data processing services provided by a third party provider, they will benefit from more effective switching themselves, while simultaneously invariably bound by this Regulation's obligations for what pertains to their own service offerings."

Art. 24(1) lists three clauses which to include in the contract between customer and originating provider on a mandatory basis. In anticipation of the Rulebook relating to cloud services (originally expected for Q2 2022[53]), Rec. 75 goes further than mere convergence and encourages the reliance on standard contractual clauses, among other tools for compliance, to foster both legal certainty and trust in data processing services.

In its introductory sentence, Art. 24(1) requires that a written contract be concluded. As *Leistner* and *Antoine* propose, any agreement in electronic form should be sufficient to meet this requirement.[54]

Switching Within a 30-day Transition Period

As per Art. 24(1)(a) the first clause to be inserted in service agreements pertains to the way in which the datasets at issue can be extracted from the originating service upon a customer's valid request. Interestingly, the Commission affords a choice here between cross-platform data exports and transfers to a so-called on-premise system. The Data Act explicitly subscribes then to the idea of making available digital assets via on-premise (*in situ*) portals operated by the originating service. This has been favoured by some economists, particularly for business customers, to overcome information asymmetries to their detriment since multidimensional information is by and large presented in its full context instead of being packaged and exported.[55] Should providers and data subjects as (non-business) customers exceptionally agree to opt for *in-situ* access, such an arrangement is bound to defeat the purpose of direct data exports from one provider to another under Art. 20(2) GDPR and would raise questions whether data subjects' right to data portability can be partially signed away under the Data Act. Art. 1(3) points to the contrary for the provisions of the Proposal are meant to complement, not modify

---

[53] Commission, 'A European Strategy for Data' COM(2020) 66 final, p. 18.

[54] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 114 (referencing Art. 1:301(6) of the Principles of European Contract Law); similarly, see Geiregat, S. 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, p. 39-40 at para. 41 (advocating for the phrase "durable medium").

[55] Martens, B. / Parker, G. / Petropoulos, G. / van Alstyne, M., Towards Efficient Information Sharing in Network Markets (TILEC Discussion Paper DP 2021-014), 2 November 2021), p. 21.

the right to data portability pursuant to Art. 20 GDPR.[56]. Moreover, referring to on-premise systems as an avenue for "porting" data, applications and other digital assets unduly conflates cross-platform portability and on-site transfers where no migration to a different IT infrastructure occurs. Puzzlingly, the Council Presidency now has given "on-premise" the meaning of "a digital data processing infrastructure operated by the customer itself to serve its own needs".[57] Such an understanding of *in-situ* access (denoting no migration) is hard to square with processing originally taking place on the infrastructure of the originating service, from which data sets would have to be exported off-site (*ex-situ*) to the customer-operated platform.

In a similar vein, *Schnurr* points out the incoherent use of the terms "data portability" and "interoperability" in Chapter VI on the whole and underscores the need to differentiate between one-off data exports and the migration of the underlying infrastructure as a prerequisite to what he labels "service portability".[58] Indeed, both types of transfer – data sets vs. the associated programs and cloud architecture – vary significantly in both scope and effect. For the sake of conceptual clarity, the legislator should therefore consider a distinction between service portability and "mere" data portability instead of pooling them together under the heading of "porting".[59]

Art. 24(1)(a) goes on to mandate that originating providers should offer assistance (in other words, migration support) or even take steps to complete the switching process on behalf of the customer while ensuring full continuity of their services for a transition period of up to 30 days. Essentially, originating providers have to carry out a form of "exit management"[60] for their customers switching to a destination service. However, Rec. 74 makes it clear that the duty to assist customers does *not* require providers

> "to develop new categories of services within or on the basis of the IT-infrastructure of different data processing service providers to guarantee functional equivalence in an environment other than their own systems."

Exportable Data and Applications

The types of data which are subject to cross-platform switching or on-premise transfers must be specified in a dedicated contractual clause (Art. 24(1)(b)). At a minimum, datasets imported by the customer at the start of the service agreement as well as data and meta-data created in the course of using the service are included. Default categories on the subject-matter of data exports and transfers set out within the legislative text are a welcome guidance for both customers making switching requests and for data processing services seeking to comply with them. However, whether the term used in Art. 24(1)(a) – "data generated directly or indirectly by the customer" – is co-extensive with data "imported" and "created by the customer and by the use of the service" as per Art. 24(1)(b) cannot be unambiguously determined. What seems

---

[56] Council Presidency 2022/0047(COD) – 14019/22, p. 35, adds the following limitation to Chapter II rights here (thus making a general point of provisions such as Art. 20(4) GDPR): "[…] and shall not adversely affect data protection rights of others".

[57] Council Presidency 2022/0047(COD) – 14019/22, p. 37.

[58] Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, 2022, pp. 11 et seq.

[59] See below p. 23 on Art. 29.

[60] Bomhard, D. / Merkle, M., *RDi* 2021, 168 (175).

comparatively more certain is the inclusion of data co-generated by the customer and one or more third parties (i.e., without the involvement of the originating provider).[61]

The Council Presidency, by way of a newly created Art. 24(1)(ba), makes an admission to originating providers' "business secrets" that could be revealed by disclosing metadata specific to the internal functioning of the originating service. It accordingly recommends inserting a mandatory clause into the contract that specifies, in exhaustive fashion, the categories of metadata in connection to which a risk of breaching trade secrets manifests itself.[62] *Schnurr* favours this exemption not only to protect trade secrets, but also with regard to data sets the contents of which enjoy IP protection.[63] While the amendment put forth by the Council Presidency would entail a prohibition on delaying or impeding the switching process[64], the exercise of IP rights by the originating provider could easily amount to an all-out obstruction of migrating to the destination service where the excluded categories of meta-data are not clearly specified.

After the transition period under Art. 24(1)(a) has elapsed, a further 30 days (or more) must be given to customers so that they can retrieve applicable datasets (Art. 24(1)(c)). As confirmed by Rec. 74, this provision is without prejudice to the concomitant right of retrieval found in Art. 16(4) of the Digital Content Directive which therefore applies alongside it to digital content.

Grounds for Extending the Transition Period

Finally, providers can extend the 30-days transition period prescribed by Art. 24(1)(a) to up to 6 months on the grounds of technical unfeasibility for a switching process to conclude within that time frame (Art. 24(2)). Broadly reminiscent of Art. 12(2) GDPR, detailed reasoning for the delay of the switching process must be given within 7 working days of receiving the switching request. In the view taken by the Council Presidency, customers should also be entitled to request an extension of the transition period – notably, without being restricted to a maximum time span of 6 months – on their own terms and initiative (proposed Art. 24(3)).[65]

The extension of the transition period capped at 6 months has drawn criticism by the ITRE Draft Report for not being workable in more complex cases, e.g. when moving fully integrated enterprise IoT platforms.[66]

Further Mandatory Contractual Terms?

In its compromise text, the Council Presidency seeks to introduce a couple of additional terms that appear geared towards greater customer protection, security and confidentiality of data.[67] The *first* would, in a newly created Art. 24(1)(a)(3), lay down the security of the data sets

---

[61] Geiregat, S. 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, p. 31 at para. 32.

[62] Council Presidency 2022/0047(COD) – 14019/22, p. 56.

[63] Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, 2022, p. 15; *contra* Geiregat, S. 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, p. 38 at para. 40 ("That is to say that the targeted objective of preventing vendor lock-ins could be considered to outweigh the provider's interest in IP protection, save in cases of abuse").

[64] Council Presidency 2022/0047(COD) – 14019/22, p. 56.

[65] Council Presidency 2022/0047(COD) – 14019/22, p. 57.

[66] ITRE PE732.704, p. 55.

[67] Council Presidency 2022/0047(COD) – 13342/22, p. 57.

concerned in the contract during both during transport and during the period for retrieval under Art. 24(2)(c).

The *second* clause, which the Council Presidency enumerates in Art. 24(1)(d), would require the erasure of "customer data" at the same time that the window for retrieval has come to a close – and only if the "porting process" has been completed successfully by then.[68] The term "customer data" is without any definition in the Proposal, and should hence be aligned with the language used elsewhere in the same provision (namely, in Art. 24(1)(a) and Art. 24(1)(b)).[69] To ensure coherence within the Proposal, a clarification in the Recitals should take note of the fact that this contractual agreement on erasure complements the data subject right under Art. 17 GDPR in applicable cases.[70]

The *third* clause, the substance of which is laid down in a new Art. 24(1(e), would fulfil an auxiliary purpose next to Art. 24(1)(b): accordingly, originating providers would be bound to maintain and refer the customer to a self-hosted (!), up-to-date online register holding details on the data structures and data formats available for exporting the data sets in scope.[71]

Interplay with the Digital Content Directive

The contractual arrangements to be taken in accordance with Art. 24(1) are "[w]ithout prejudice to Directive (EU) 2019/770". The uncertainties of such a generic statement of both instruments being applicable to the same set of circumstances have spurred different proposals on how to achieve a workable complementary relationship between the Data Act and the Digital Content Directive.

In the view endorsed by the MPIIC, both laws should not apply in parallel. Because Art. 24 offers a greater level of interoperability and technological governance, it should exclusively apply to digital content, including in B2C relations, thereby pre-empting the Digital Content Directive as the less "ambitious" porting regime.[72] The members of CiTiP concur in the result that Art. 24 constitutes a *lex specialis* to the Digital Content Directive, finding that Art. 11 et seq. of the Directive are not suitable for the intricacies of switching operations.[73] Conversely, *Geiregat* argues for dual application in the B2C sphere, with greater consumer protection in effect.[74]

Proposed Amendments:

– Reassess the conformity of on-premise transfers with the right to data portability in case data subjects are customers and, if applicable, eliminate on-premise transfers in the B2C sphere.

[68] Council Presidency 2022/0047(COD) – 14019/22, p. 57.

[69] See above p. 10.

[70] Cf. Rec. 35, accompanying Art. 6(1).

[71] Council Presidency 2022/0047(COD) – 14019/22, p. 57.

[72] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 65 n. 177.

[73] Ducuing, C. / Margoni, T. / Schirru, L. (Ed.), *CiTiP Working Paper* 2022, 62.

[74] Geiregat, S. 'The Data Act: Start of a New Era for Data Ownership?' (SSRN pre-print), 2022, pp. 37 et seq. at para. 39.

– Establish Art. 24 as *lex specialis* overriding the provisions of the Digital Content Directive for switching between cloud services – possibly as a new paragraph of Art. 1.

Art. 24(1)

– Replace the term "porting" in point (a) of Art. 24(1) with "transfer", thereby avoiding confusion with the settled concept of porting (personal) data under Art. 20(1)-(2) GDPR.

– Calibrate the wording of point (a) with point (b) of Art. 24(1), making sure that data being "generated directly or indirectly by the customer" (point (a) are broadly co-extensive or share a clear overlap with data being "imported" and "created" by the customer (point(b)).

Rec. 72

– Add to Rec. 72 a new second sentence to avoid doubt that agreements made in electronic form satisfy the criterion of a written contract.

3. Reduced Switching Charges (Art. 25)

On top of data-induced vendor lock-in, customers with large quantities of data have so far been discouraged to switch to a new data processing service because providers often charge significantly for the retrieval of data (so-called data egress costs) and for their onwards transfer (so-called transport fees).[75] Art. 25 aims to gradually put an end to these economic barriers.

For a period of three years after the Data Act has come into force, providers may impose reduced charges compared to the amount they have previously billed their customers for switching to a new service (Art. 25(2)). As evidenced by Art. 25(3), these reduced charges shall only cover the costs for providers directly linked to the switching process, hence eliminating commercial incentives to make a profit at the expense of their customers.

Once the transitional three years have passed, switching charges shall be abolished altogether under Art. 25(1). In order to reach this target, the Commission may adopt delegated (i.e. tertiary) legislation to monitor the progress of diminishing switching charges during the 3-years transition period (Art. 25(4)). Conversely, it does not follow that the Commission can object at that time to any fluctuation of switching charges within the cost-covering threshold.

The IMCO Draft Opinion seeks to accelerate the total withdrawal of switching charges primarily for consumers (which lacks a definition in the Proposal as of yet, but could be borrowed, e.g., from Art. 2(6) of the Digital Content Directive). Under a redrafted Art. 25(1), the abolition of switching charges would be tied to the date when the Data Act enters into force.[76] For non-consumer customers, charges would have to be reduced from that date onwards.[77]

Going in the opposite direction, *Leistner* and *Antoine* point out the financial burden linked to complex switching operations, calling into question the layered 'sunset period' for switching

[75] Commission, 'Switching of Cloud Services Providers' (2018), pp. 42-46.

[76] IMCO PE736.701, p. 41.

[77] IMCO PE736.701, p. 41.

charges.[78] According to *Schnurr*, the burden would especially put a strain on smaller providers of cloud services as they would typically struggle to compensate for the lost switching charges through other revenue streams.[79] Following this line of reasoning, asymmetries in the financial capabilities of differently sized enterprises could be remedied by allowing SMEs (especially given their favourable treatment elsewhere in the Proposal[80]) to continue to claim reduced switching charges even after the sunset period under Art. 25(2) has elapsed.

Proposed Amendments:

Art. 25(2)

– Add a second sentence that empowers the Commission to set a prolonged period when reduced switching charges may be demanded where the originating provider is an SME

4. Technical Enablers of Switching (Art. 26)

Art. 26 strikes a key distinction amongst data processing services. For providers that limit their offering to supplying physical or virtual computing resources as infrastructure, functional equivalence as sketched in Art. 23(1)(d) must be ensured in the use of the new service (Art. 26(1)).[81] From what Rec. 76 attributes to PaaS and SaaS business models, one may infer *e contrario* that Art. 26(1) primarily targets IaaS (infrastructure-as-a-service) data processing. The classic example of cloud storage stands to reason where access to further software (i.e. beyond the user account for obtaining access to the stored data) is generally not granted. Within these boundaries, a disconnect with the objective set in Art. 23(1)(d) as observed by *Leistner* and *Antoine* should not arise for output on the core elements of IaaS will mostly be relatively easy to align.[82] The Council Presidency has nonetheless regarded the wording of Art. 26(1) ("should ensure") as too far-reaching and has moved to replace it with a less invasive principle of cooperation between the provider of the originating service and the provider of the destination service.[83] Relatedly, *Schnurr* argues that the "best effort" in supplying the exportable data sets is all that can be expected from the originating provider so that the output on the destination service can qualify as functionally equivalent.[84] Both suggestions rightly touch upon the legal maxim of *nemo ultra posse obligatur:* the originating provider can not be tasked with an obligation whose fulfilment (by the destination provider) they do not ultimately control.

[78] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 115.

[79] Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, 2022, p. 15.

[80] Cf. e.g. Art. 7(1), Art. 9(2) and Art. 13.

[81] Critical of Art. 23(1): IMCO PE736.701, p. 43.

[82] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 113 et seq.

[83] Council Presidency 2022/0047(COD) – 13342/22, p. 58.

[84] Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, 2022, p. 17.

More complex data processing services such as PaaS, SaaS, and edge computing services need not cater for functional equivalence, but have to set up open interfaces, most prominently Application Programming Interfaces (APIs), at no additional cost to customers (Art. 26(2)). Intellectual property held with respect to the technical means for switching should consequently not be a limiting factor to the data migration at hand.[85] Furthermore, under Art. 26(3) providers have to align with open interoperability specifications or European standards for interoperability[86] that have been developed in accordance with the European Standardisation Regulation (EU) 1025/2012 (cf. Rec. 76). Should no standards of this sort exist as of yet, Art. 26(4) constitutes a fall-back provision whereby all (co-)generated data shall be exported in a structured, commonly used, and machine-readable format. The latter part of Art. 26(4) mirrors Art. 20(1) GDPR, which does *not* impose interoperability mandates though as per Rec. 68 GDPR. This provision, which does not have a counterpart in Chapter II, responds to the problem, frequently voiced during the consultation period, of lacklustre standardisation as to data formats.[87]

Again, the hazy notion of "generated" data (cf. Rec. 17) might obstruct a clear understanding of which datasets are to be disclosed in practice.

Proposed Amendments:

Art. 26(1)

- Qualify Art. 26(1) in the sense that the originating provider should work towards functional equivalence on the destination service only to the extent to which this is (remotely) possible to them
- Consequently, adjust the definition for functional equivalence in Art. 2(14), which could be done through Rec. 74

Rec. 76

- Insert a new initial sentence into Rec. 76: "For cloud services operating solely at the IaaS (infrastructure-as-a-service) level, the supply of infrastructural elements such as servers, networks or virtual machines should entail functional equivalence of the output on the data retrieved."

[85] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 66 n. 180.

[86] See below p. 23.

[87] Podzsun, R., Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, 2022, p. 45.

IX. Transfer of Non-Personal Data to Third Countries (Art. 27)

Chapter VII ('Unlawful International Governmental Access and Transfer of Non-Personal Data', Art. 27) aims to prevent unlawful third-party access to non-personal data held in the Union by data processing services offered on the Union market through technical, legal, and organisational safeguards.[88] Rec. 77 argues respectively that "third countries may adopt laws, regulations and other legal acts that aim at directly transferring or providing governmental access to non-personal data located outside their borders, including in the Union."

The provision of Art. 27 recalls similar provisions first in the GDPR (Art. 44-50) for personal data and then in the DGA (Art. 31); the latter being concerned with non-personal data as well as with data sharing services, public sector bodies, natural or legal persons with the right to re-use data and recognised data altruism organisations. Generally, the structure of Art. 27 mirrors the approach of Art. 31 DGA.

Art. 27 only addresses data held by data processing services according to Art. 2(12). Thus, other activities of a company that is not only active as a data processing service are not covered by Art. 27.[89] They might, however, fall under the scope of the GDPR or the DGA (Art. 31).

The IMCO Draft Opinion proposes to change "data processing" to "cloud switching".[90]

The general approach of Art. 27 is not free of doubt. There is the risk that the opposing objectives of Art. 27 and Art. 23-26 may create an imbalance between enabling switching between data processing services, which means a transfer of data, and restricting data transfers in the direction of non-EU countries. It is therefore argued that Art. 27 might not be in line with the principal objective of the Data Act to enhance data sharing.[91]

On one hand, it is questionable whether Art. 27 is necessary and justified concerning non-personal data, where its prime objective is not the protection of fundamental rights and freedoms of the data subject.[92] On the other hand, non-personal data can have implications for the public interest, for example related to public security, that might justify the restriction of international data transfer.

In practice, it might become difficult to determine, whether Art. 44-50 GDPR or Art. 27 apply, as firstly personal and non-personal data may be mixed in datasets and secondly it is increasingly hard to distinguish personal and non-personal data.[93]

1. Preventing International Transfer and Governmental Access (Art. 27(1))

Where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, Art. 27(1) obliges the providers of data processing services to take all reasonable technical, legal, and organisational measures, including contractual arrangements,

---

[88] Commission, COM(2022) 68 final Explanatory Memorandum, p. 16.

[89] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 69 n. 189.

[90] IMCO PE736.701, p. 47.

[91] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 69 n. 189.

[92] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 69 n. 190.

[93] Ducuing, C. / Margoni, T. / Schirru, L. (Ed.), *CiTiP Working Paper* 2022, 69.

in order to prevent international transfer or governmental access to non-personal data held in the Union.

In Rec. 78 "the encryption of data, the frequent submission to audits, the verified adherence to relevant security reassurance certification schemes, and the modification of corporate policies" are given exemplary as measures that should be taken by the providers of data processing services.

The MPIIC argues that this provision could lead to data processing service providers completely refraining from transferring data to countries outside of the EU.[94] The MPIIC understands its aim as protecting the respect of any law on the EU and national level. As no specific event as for example a judgement (as do (2) and (3)) is required, it could potentially affect the entire business of a globally operating service provider.[95] According to this interpretation the provision of Art. 27(1) could require the monitoring of the content of all data, although a provider of data processing services is not a content provider.[96] Firstly, this would lead to immense costs for the service provider, while it might not even be technically possible to monitor all the data.[97] Secondly, the service provider would need the customer to agree to the monitoring of the data in the contract.[98] Thus, it could *de facto* be preferable that service providers refrain from transferring data to third countries altogether.

The assessment of this provision depends in particular on the understanding of "create a conflict with union law". This requirement is seen as especially problematic.[99] The MPIIC interprets it as requiring less than a violation of the law by the service provider.[100] Thus, this rule would establish a "contributory liability" and require the service provider to prevent a violation of the law by its customer.[101] It could be understood to protect interests that are already protected by other fields of law, which already contain a distinction on who is liable and who is not, based on a specific balance of interest.[102] Art. 27(1) could put potentially the specific legislative weighing of interests aside and create new obligations for the service providers.[103]

However, a different interpretation of Art. 27(1) seems possible. It can be argued that the requirement – not to create a conflict with Union law or national law – has to be seen in the context of data (protection) transfer rules (as Art. 44 et seq. GDPR). Consequentially, it has to be asked which kind of transfers are actually forbidden. Where Art. 44 openly puts a general ban (with the exceptions in Art. 45 et seq. GDPR) on transfers, Art. 27(1) obviously takes a different stand for non-personal data (which generally are allowed to flow freely). The transfer shall only be restricted in specific cases – targeted at the process of transfers (not at any field

[94] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 73 n. 197.

[95] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 73 n. 198, 199.

[96] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 73 n. 200.

[97] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 73 n. 200.

[98] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 73 n. 200.

[99] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 75 n. 206.

[100] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 75 n. 206.

[101] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 75 n. 206.

[102] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 75 n. 206.

[103] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 75 n. 206.

of law). Along these lines, it seems favourable to understand Art. 27(1) to be referring only to legislation specifically prohibiting data transfer or access.[104]

In favour of such an interpretation does not only speak the far-too-burdensome consequence of the establishing of a "contributory liability" as described by the MPIIC. It must also be stressed that Art. 27 would otherwise contradict the Data Act's aim of enhancing data sharing.

However, it is the unspecific wording "create a conflict with Union law or national law" itself, that gives reason for such a far-reaching interpretation. Hence, it should be clarified, that Art. 27(1) refers to legislation specifically prohibiting data transfer or access to thirdc countries.

The JURI Draft Opinion proposes to change "create a conflict" to "be in contravention" which would give a clearer and stricter understanding of this requirement in Art. 27(1).[105] The IMCO Draft Opinion proposes a new Art. 27(1a) according to which – where the data transfer is subject to appropriate safeguards as defined under Art. 46 GDPR – the conditions set out in Art. 27(1) shall be presumed fulfilled.[106] It is, however, questionable whether the safeguards for personal data should be applied to non-personal data.

The IMCO Draft Opinion proposes a new Art. 27a, allowing the Commission to adopt a list of third country jurisdictions where international transfer or governmental access to non-personal would create a conflict with Union law or the national law of the relevant Member State.[107] It also proposes criteria which should be considered: conflicting regulations including on data protection, public security or national security; access to the reasoned objection procedure; the level of risk to lose the confidentiality of commercially sensitive data; international commitments; third country adequacy recognition under Art. 45 GDPR.[108]

It has to be stressed that further clarification on potential conflicts with Union or national law is needed. It seems, however, in many ways unclear – and is in substance rather unjustified – why (personal) data protection law and especially an Art. 45 GDPR-adequacy status should be considered regarding the transfer of non-personal data.

Lastly, Art. 27(1) requires far reaching measures only limited by the test of reasonableness.[109] It should be clarified that this also encompasses the requirement of technical feasibility.

2. Enforcement of Foreign Judgements and Decisions (Art. 27 paras. 2 and 3)

Judgments of courts or tribunals or decisions of other judicial or administrative authorities, including law enforcement authorities in third countries requiring such transfer or access to non-personal data should be enforceable when based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, Art. 27(2) and Rec. 77.

---

[104] See also in the context of the parallel rule of Art. 31 DGA Hennemann, M., in: Specht-Riemenschneider, L./Hennemann, M., Data Governance Act, 2023, Art. 31 DGA, forthcoming.

[105] JURI PE736.696, p. 51.

[106] IMCO PE736.701, p. 47.

[107] IMCO PE736.701, p. 50.

[108] IMCO PE736.701, p. 50.

[109] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 73 n. 200.

If such an agreement exists, it sets a clear legal standard and protects service providers from taking on the role of law enforcer.[110] Rec. 77 further explains that

> "in other cases, situations may arise where a request to transfer or provide access to non-personal data arising from a third country law conflicts with an obligation to protect such data under Union law or national law, in particular as regards the protection of fundamental rights of the individual, such as the right to security and the right to effective remedy, or the fundamental interests of a Member State related to national security or defence, as well as the protection of commercially sensitive data, including the protection of trade secrets, and the protection of intellectual property rights, and including its contractual undertakings regarding confidentiality in accordance with such law."

In the absence of international agreements regulating such matters and compliance with the decision would risk putting the addressee in conflict with Union law or the relevant national law, transfer or access should only be allowed according to Art. 27(3), if

> (a) it has been verified that the third country's legal system requires the reasons and proportionality of the decision to be set out, that the court order or the decision is specific in character, (…) and
>
> (b) the reasoned objection of the addressee is subject to a review by a competent court in the third country and
>
> (c) the competent court or tribunal issuing the decision or judgement or reviewing the decision of an administrative authority is empowered under the law of that country to take duly into account the relevant legal interests of the provider of the data protected by Union law or national law of the relevant Member State.

It seems unclear, when the threshold "would risk putting the addressee at conflict with…" is met. The JURI Draft Opinion proposes again to change "create a conflict" to "be in contravention" in Art. 27(3).[111]

To determine, whether these conditions are met, the addressee of the decision can ask the competent authorities, which alleviates the burden on the service provider.[112] It remains unclear, whether this also concerns the determination, whether there is a conflict with EU or national law according to Art. 27(1)[113]. The wording "these conditions" without further specification, argues for the interpretation that the determination of a conflict with EU or national law is also included.[114] It is furthermore unclear whether the issued opinions of the competent authorities are binding or not.[115] Thus it should be clarified whether, if the competent authority concludes

---

[110] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 70 n. 193.

[111] JURI PE736.696, p. 42.

[112] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 71 n. 194.

[113] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 71 n. 195.

[114] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 71 n. 195.

[115] Ducuing, C. / Margoni, T. / Schirru, L. (Ed.), *CiTiP Working Paper* 2022, 66.

that these conditions are not met, the addressee of the decision is obliged to deny the transfer of data.[116]

The Council Presidency proposes, to change "relevant competent bodies or authorities pursuant to this Regulation" to "relevant national body or authority competent for international cooperation in legal matters".[117]

It is welcomed by *Leistner* and *Antoine* that the European Data Innovation Board (to be established according to Art. 29 DGA) shall advise the Commission on developing guidelines on the assessment of whether the conditions laid down in Art. 27(3) are met.[118] However, the IMCO Draft Opinion proposes to delete this subparagraph altogether.[119]

If these conditions are met, the provider of data processing services shall provide the minimum amount of data permissible in response to a request, Art. 27(4). The wording of this provision should be adjusted to clarify, that the principle of data minimisation relates to its informational content rather than to the amount of data.[120]

The JURI Draft Opinion proposes a new Art. 27(4a) that where the data processing service provider has reason to believe that the transfer of or access to non-personal data may lead to the risk of re-identification of non-personal data, or anonymised data, the provider shall request the relevant bodies or authorities for authorisation before transferring or giving access to data.[121]

According to Art. 27(5) the provider of data processing services should inform the data holder about the existence of a request of an administrative authority in a third country to access its data before complying with its request, except in cases where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity. The provision should be extended to also cover requests by foreign courts.[122]

Rec. 77 adds, that the provider of data processing services should,

> "wherever possible under the terms of the data access request of the third country's authority, be able to inform the customer whose data are being requested in order to verify the presence of a potential conflict of such access with Union or national rules, such as those on the protection of commercially sensitive data, including the protection of trade secrets and intellectual property rights and the contractual undertakings regarding confidentiality."

---

[116] Ducuing, C. / Margoni, T. / Schirru, L. (Ed.), *CiTiP Working Paper* 2022, 66.

[117] Council Presidency 2022/0047(COD) – 14019/22, p. 59.

[118] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 116; BDI Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, p. 21.

[119] IMCO PE736.701, p. 49.

[120] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 72 n. 196.

[121] LIBE PE737.389, p. 59.

[122] Max Planck Institute for Innovation and Competition, Position Statement, 2022 p. 72 n. 195.

The broad term "providers of data processing services" also includes cloud storage providers, thus leading to an efficient protection of data which is not stored in in-house infrastructure.[123]

Leistner and *Antoine* see the conditions for transferring or making data available laid down in Art. 27(3) as an adequate and structured framework for protecting non-personal data against inadequate international transfer or governmental access[124]. In contrast, the BDI criticises, that it implements a level of protection for non-personal data which is usually only known for the protection of personal data as protection of fundamental rights[125].

Personal data as part of fundamental rights should be protected against the transfer to countries where the law fails to grant equivalent protection.[126] However, this does not necessarily apply to non-personal data, which is not linked to fundamental rights and where no personal interests argue against cross-border data transfers.[127] While the restriction on cross-border transfer in the GDPR complies with its general objective to protect personal data, Art. 27 stands in opposition to the objective of the Data Act to enhance data sharing.[128]

However, Art. 27 applies a framework for the international transfer of and access to data that is different from the framework in Art. 44-50 GDPR. And while the transfer of non-personal data does not affect personal interests, it may affect national security interests, which can justify restrictions on international data transfer and access.

Proposed Amendments:

- Art. 27 should be reconsidered regarding its implication for switching between data processing services according to Art. 23-26 and its compatibility with the aim of the Data Act to enhance data-sharing.
- The criteria to determine a conflict with Union or Member State law shall be clarified.
- Consider the proposal of the IMCO Draft Report to allow the Commission to adopt a list of third county jurisdictions where international transfer or governmental access to non-personal would create a conflict with Union law or the national law of the relevant Member State.

Art. 27(1)

- Consider to change "create a conflict" to "be in contravention".
- Clarify that this depends on the existence of legislation specifically prohibiting data transfer or access.

[123] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 115.

[124] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 115.

[125] BDI Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, p. 21.

[126] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 69 n. 190.

[127] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 69, 70 n. 190.

[128] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 70 n. 190.

– Clarify that the test of reasonableness encompasses the requirement of technical feasibility.

Art. 27(3)

– Clarify whether the opinion issued by the competent authority is binding and would oblige the service provider to deny the transfer of data.

– Consider to change "create a conflict" to "be in contravention".

Art. 27(4)

– It should be clarified that the principle of data minimisation relates to its informational content rather than the amount of data.

Art. 27(5)

– Its scope should be extended to also cover requests by foreign courts.

X. Interoperability (Art. 28-30)

Chapter VIII ('Interoperability', Art. 28-30) provides for essential requirements to be complied with regarding interoperability for operators of data spaces and data processing service providers as well as for essential requirements for smart contracts. Further technological convergence is envisioned through the proposed development of open interoperability specifications and European standards for the interoperability of data processing services.[129]

The Commission's Rationale for Taking Regulatory Action

The Commission concurs with findings made by the OECD that a lack of common standards constitutes one of the most pressing barriers to data sharing and re-use.[130] Rec. 76 notes that in the absence of market dynamics towards harmonised technical specifications, European standardisation bodies on the basis of Regulation (EU) 1025/2012 can intervene at the behest of the Commission. Rec. 79 puts this into concrete terms for semantic interoperability.

1. Interoperability Requirements within Data Spaces (Art. 28)

Art. 28(1) enumerates, in rather open-ended and generic fashion (as is conceded towards the end), four categories of essential requirements to facilitate the interoperability of data, data sharing mechanisms, and between services.

Sub (a), key properties of the data set at issue relating to its content, (re-)use, and quality have to be communicated so that recipients can find, access, and use the data set. (b) mandates that formal aspects of the data set, most notably their format and data taxonomies, shall be disclosed in a publicly available and consistent manner. (c) singles out application programming interfaces (APIs) as a crucial way to access data and demands their specification so that real-time access in a machine-readable format is possible. Finally, (d) considers the interoperability of so-called 'smart contracts'.

The MPIIC embarks on an in-depth analysis of the ramifications of intellectual property rights held with regard to APIs, as they are mentioned by Art. 28(1)(c).[131] Ultimately, a sweeping exemption, modelled after Art. 35, is suggested for IP rights over APIs in the case of access within data spaces.[132]

Now that a Regulation for a European Health Data Space has been announced[133], the umbrella term, namely "Common European Data Spaces", should be fleshed out by way of a legislative definition[134] To achieve consistency with the Data Governance Act (DGA) on the matter, the legislator could restate the definition given in Art. 30(h) DGA, which frames Common European Data Spaces as "purpose- or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data for, *inter alia*, the development of new products and services, scientific research or civil society initiatives".

---

[129] Commission, COM(2022) 68 final Explanatory Memorandum, p. 16.

[130] SWD(2022) 34 final (n 38), p. 22.

[131] Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 82 n. 223 et seq.

[132] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 82 n. 226.

[133] See COM(2022) 197 final.

[134] *Ex multis*, Ducuing, C. / Margoni, T. / Schirru, L. (Ed.), CiTiP Working Paper 2022, p. 15.

In a similar fashion, the Council Presidency seeks to elucidate the notion of operators within such data spaces, defining them as "legal persons that facilitate or engage in data sharing within and across the common European data spaces".[135] Once the other iterations of sectoral data spaces as envisioned by the Commission's Data Strategy have unfolded[136] and the European Data Innovation Board has commenced its work under Art. 30(f)-(h) of the Data Governance Act, it will be apparent whether this definition is sufficient in detail.

Proposed Amendments:

- Consider a cross-reference to Art. 30(h) DGA for the definition of "Common European Data Spaces"
- Integrate the Council Presidency's definition of "operators within data spaces" into a new No. under Art. 2
- Consider more seamless access through APIs by relaxing IP protection in the situations envisioned by Art. 28 for data spaces.[137]

2. Interoperability for Data Processing Services (Art. 29)

Art. 29 expands on interoperability requirements in the context of data processing services, i.e. cloud offerings as targeted by the switching requirements of Chapter VI. Due to the inherent *nexus* with said Chapter (encapsulated by Art. 26(4)), the MPIIC recommends moving Art. 29 there.[138]

The first paragraph of Art. 29 aims at establishing a three-fold technical convergence between data processing services, specifically towards interoperability as defined in Art. 2(19), portability as sketched by Art. 24(1)(a), and functional equivalence as defined in Art. 2(14).

The second paragraph reproduces, to the letter, the standards advanced by the International Standards Organization (ISO) with respect to cloud interoperability and portability.[139]

Art. 29(4) and Art. 29(5) confer upon the Commission rulemaking powers to issue European standards for the interoperability of data processing services.

3. Common Standards for Smart Contracts (Art. 30)

Art. 30 concludes the efforts for standardisation and interoperability under Chapter VIII by introducing smart contracts. Their conception as computer programs pursuant to the definition given in Art. 2(16) has been criticised as violating the principle of technological neutrality.[140]

---

[135] Council Presidency 2022/0047(COD) – 14019/22, p. 38.

[136] COM(2022) 66 final, p. 22.

[137] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 82 n. 226.

[138] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 67 n. 181.

[139] ISO-Norm ISO/IEC 19941:2017, Information technology — Cloud computing — Interoperability and portability, pp. 36 et seq.; cf. Rec. 76.

[140] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 84 n. 234.

The compromise text published by the Council Presidency accordingly broadens the concept to include other tools for the automated execution of data sharing agreements.[141]

The first paragraph deems four characteristics essential for smart contracts: robustness, safe termination and interruption, data archiving and continuity, and access control. Of these, the possibility to interrupt (Art. 30(1)(b)) the execution of the self-executing protocol underlying the smart contract would disturb the immutability of the ledger and thereby thwart a key advantage of the distributed ledger technology (DLT).[142]

[141] Council Presidency 2022/0047(COD) – 13342/22, p. 61.

[142] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 85 n. 235.

XI. Implementation and Enforcement (Art. 31-34)

Chapter IX ('Implementation and Enforcement', Art. 31-34) lays down the implementation and enforcement framework with regard to competent authorities in each Member State, including a complaints mechanism and co-operation with data protection authorities.[143]

Chapter IX focuses on public enforcement and fails to address private enforcement, although a central part of the Data Act regards contractual relationships. The mentioning of collective actions in Rec. 82 implies private enforcement and Art. 10(5) assumes that national courts could take cases on FRAND litigation. Still, the possibility of private enforcement should be addressed directly in the regulation.

1. Competent Authorities (Art. 31)

"In order to ensure the efficient implementation of this Regulation, Member States should designate one or more competent authorities." Art. 31(1), Rec. 81. Art. 31(2) further defines which authorities are competent:

> (a) the independent supervisory authorities responsible for monitoring the application of the General Data Protection Regulation should also be responsible for monitoring the application of the Data Act insofar as the protection of personal data is concerned.
>
> (b) for specific sectoral data exchange issues related to the implementation of this Regulation, the competence of sectoral authorities should be respected
>
> (c) the national competent authority responsible for the application and enforcement of Chapter VI of this Regulation should have experience in the field of data and electronic communications services

When a member state designates more than one competent authority, which monitor these distinguished yet overlapping sectors, their competences have to be distributed carefully between them.[144]

The JURI Draft Opinion proposes a Data Coordinator instead of the competent authority. Thus it also proposes a new corresponding title for Art. 31 and to change "one or more competent authorities" in Art. 31(1) to "an independent competent coordinating authority (data coordinator), to delete "Member States may establish one or more new authorities or rely on existing authorities" and instead add "for coordinating the activities entrusted to that Member State, for acting as the single contact point towards the Commission, with regard to the implementation of this Regulation and for representing the Member State at the European Data Innovation Board, as referred to in Article 31a."[145] Accordingly, in the following paragraphs and also regarding the other Articles of the Data Act Proposal, JURI proposes to replace "competent authorities" with "data coordinator".

JURI further proposes to change the first sentence of Art. 31(2) from "Without prejudice to paragraph 1 of this Article: ..." to "the data coordinator shall ensure cooperation among the national competent authorities that are responsible for monitoring of other Union or national

---

[143] Commission COM(2022) 68 final Explanatory Memorandum, p. 16.

[144] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 117.

[145] JURI PE736.696, pp. 53 et seq.

legal acts in the field of data and electronic communications services, namely: …"[146] JURI also proposes to delete Art. 31(2)(c).[147]

Member states should clearly define the tasks and powers of the competent authorities which according to Art. 31(3) should include:

> (a) promoting awareness among users and entities falling within scope of this Regulation of the rights and obligations under this Regulation;
>
> (b) handling complaints arising from alleged violations of this Regulation, and investigating, to the extent appropriate, the subject matter of the complaint and informing the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another competent authority is necessary;
>
> (c) conducting investigations into matters that concern the application of this Regulation, including on the basis of information received from another competent authority or other public authority;
>
> (d) imposing, through administrative procedures, dissuasive financial penalties which may include periodic penalties and penalties with retroactive effect, or initiating legal proceedings for the imposition of fines;
>
> (e) monitoring technological developments of relevance for the making available and use of data;
>
> (f) cooperating with competent authorities of other Member States to ensure the consistent application of this Regulation, including the exchange of all relevant information by electronic means, without undue delay;
>
> (g) ensuring the online public availability of requests for access to data made by public sector bodies in the case of public emergencies under Chapter V;
>
> (h) cooperating with all relevant competent authorities to ensure that the obligations of Chapter VI are enforced consistently with other Union legislation and self-regulation applicable to providers of data processing service;
>
> (i) ensuring that charges for the switching between providers of data processing services are withdrawn in accordance with Art. 25.

The JURI Draft Opinion proposes to add to Art. 31(3)(a) "data literacy measures and tools, raising awareness" after promoting.[148] It also proposes to add a new para. (aa) "issuing recommendations and providing advice to users and entities, in particular to micro, small and medium-sized enterprises on the implementation of this Regulation", as well as a new para. (ab) "facilitating the exchange of information and best practices among entities falling under the scope of this Regulation.[149]

---

[146] JURI PE736.696, p. 54.

[147] JURI PE736.696, p. 55.

[148] JURI PE736.696, p. 55.

[149] JURI PE736.696, p. 56.

Art. 31(3)(g) only concerns the online public availability of requests in cases of public emergencies, unlike Art. 17(2)(f) which obliges public sector bodies to make all requests publicly available online.[150] To foster transparency and coherence Art. 31(3)(g) should cover all requests in cases of exceptional need. This change is also proposed by the JURI Draft Opinion.[151] The Council Presidency proposes to add "and promoting voluntary data sharing agreements between public sector bodies and data holders".[152]

The Council Presidency proposes to add an additional Art. 31(3)(j) that the competent authorities should examine the requests for data made pursuant to Art. 14(1) in cross-border contexts.[153]

According to Art. 31(4) and Rec. 81,

> "if a Member State designates more than one competent authority, it should also designate a coordinating competent authority. Competent authorities should cooperate with each other. The authorities responsible for the supervision of compliance with data protection and competent authorities designated under sectoral legislation should have the responsibility for application of this Regulation in their areas of competence."

As a consequence of the proposal for a data coordinator, the JURI Draft Opinion proposes to delete Art. 31(4).[154]

The Commission should maintain a public register of the competent authorities based on the information the Member States should communicate, Art. 31(5).

The competent authorities shall remain free from any external influence, whether direct or indirect, and shall neither seek nor take instructions from any other public authority or any private party, Art. 31(6).

The Member States should ensure that the competent authorities are provided with the necessary resources, Art. 31(7).

The Council Presidency proposes a new para. 8 that in accordance with the Regulation (EU) 2018/1725 the European Data Protection Supervisor should be responsible for monitoring the application of Chapter V insofar as the processing of personal data is concerned.[155]

Coordination between Competent Authorities of Member States and on the Enforcement of Data Regulation

The decentralised enforcement of the Data Act by various competent authorities in the individual member states planned in Art. 31 may lead to a fragmented application and varying regional standards for data access.[156] Additional to that, the competences must be distributed

---

[150] Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 54 n. 147.

[151] JURI PE736.696, p. 56.

[152] Council Presidency 2022/0047(COD) – 14019/22, p. 64.

[153] Council Presidency 2022/0047(COD) – 15035/22, p. 70.

[154] JURI PE736.696, p. 58.

[155] Council Presidency 2022/0047(COD) – 14019/22, p. 64.

[156] BDI Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, p. 22.

between the authorities of the member states and those on the European level in such a way, that a harmonised and coordinated enforcement will not be jeopardised.[157]

Thus, *Leistner* and *Antoine* propose a so-called "meta-authority" on European level to oversee not only the implementation of the Data Act, but of the enforcement and coordination of all data-related obligations, for instance the Data Governance Act, the Digital Markets Act and the Digital Services Act.[158] This authority should be designed as an "umbrella institution" under which the different European and national institutions could exchange information, cooperate and deliver respective elements of necessary decisions, in order to reduce fragmentation.[159] We agree that additionally to the coordination between the competent authorities according to the Data Act, the coordination of the enforcement of all data-related obligations has to be addressed by the legislator.

This role could fall on the European Data Innovation Board established according to Art. 29 DGA, which already has the task of advising and assisting the Commission also on matters beyond the scope of the Data Governance Act and should facilitate the cooperation between Member States. Having this existing institution also coordinate the enforcement of other data-related regulation, such as the Data Act, would be preferable to establishing a new "meta-authority".

With the respective aim of further improving coordination at European level, the ITRE Draft Report and the JURI Draft Opinion each propose a new Art. 31a on the Role of the European Data Innovation Board[160]. According to these proposals, it should foster mutual exchange of information amongst competent authorities as well as advise and assist the Commission in all matters falling under this Regulation.[161]

JURI Draft Opinion also proposes that the data coordinators should represent the Member States on the European Data Innovation Board.[162]

The Council Presidency proposes a similar Art. 34a on the Role of the European Data Innovation Board.[163]

The Council Presidency also proposes a new Art. 31(9) concerning cooperation and mutual assistance between the competent authorities of the Member States.[164]

---

[157] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 117.

[158] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 117.

[159] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 117.

[160] Established in Art. 29 et seq. of the Data Governance Act.

[161] ITRE PE 732.704, 56 et seq.; JURI PE736.696, p. 60.

[162] JURI PE736.696, p. 60.

[163] Council Presidency 2022/0047(COD) – 14019/22, p. 66 et seq.

[164] Council Presidency 2022/0047(COD) – 14019/22, pp. 64 et seq.

Similarly, the ITRE Draft Report also proposes a new Art. 33a on mutual assistance between the competent authorities and the Commission.[165]

The Council Presidency further proposes new paras. 10 and 11 to determine to which Member State jurisdiction entities falling within the scope of the Data Act should be subject.[166]

Proposed Amendments:

- Address the coordination between competent authorities of different member states.
- Address the coordination of enforcement of all data related legislation.
- Consider which role the European Data Innovation Board could play in the implementation of the Data Act as well as the coordination between the competent authorities of the Member States.

Art. 31(3)

- Amend Art. 31(3)(g): replace "cases of public emergencies" with "cases of exceptional need".

2. Right to Lodge a Complaint with a Competent Authority (Art. 32)

In order to enforce their Data Act rights, natural and legal persons should be entitled to seek redress for the infringements of their rights under this Regulation by lodging complaints with competent authorities, Art. 32(1) and Rec. 82.

The ITRE Draft Report proposes to add a new para. 1a, that each Member State should notify the Commission and the European Data Innovation Board the provisions of national measures adopted pursuant to para. 1 without delay as well as any subsequent amendment affecting them.[167]

According to Art. 32(2) the competent authority with which the complaint has been lodged shall inform the complainant of the progress of the proceedings and of the decision taken.

Those authorities should be obliged to cooperate to ensure the complaint is appropriately handled and resolved, Art. 32(3) and Rec. 82.

The right to lodge a complaint under Art. 32 is without prejudice to any other administrative or judicial remedy, Art. 32(1), thus not precluding private remedies or enforcement.[168] It does however not address comprehensively the role of private remedies or enforcement.[169] This lack of harmonisation of private enforcement may lead to disharmony concerning claims by users, but also unfair competition law-based actions and national legislation on private remedies

[165] ITRE PE 732.704, pp. 57 et seq.

[166] Council Presidency 2022/0047(COD) – 14019/22, p. 65.

[167] ITRE PE 732.704, p. 57.

[168] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 118.

[169] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 118.

concerning the rights under the Data Act.[170] Such harmonisation could also clarify the relationship between public enforcement and private remedies.[171]

Proposed Amendment:

– The if and how of private enforcement should be expressly regulated in the Data Act.

3. Penalties (Art. 33)

The Member States should lay down rules on penalties applicable to infringements of the Data Act, which are effective, proportionate and dissuasive, and should take all measures necessary to ensure that they are implemented, Art. 33(1). Until the begin of the application of the Data Act, the Member States should notify the Commission of those rules and measures as well as of any subsequent amendment affecting them, Art. 33(2).

Additionally, Rec. 83 states that it is the task of the competent authorities to ensure that infringements of the obligations laid down in the Data Act are sanctioned by penalties:

> "When doing so, they should take into account the nature, gravity, recurrence and duration of the infringement in view of the public interest at stake, the scope and kind of activities carried out, as well as the economic capacity of the infringer. They should take into account whether the infringer systematically or recurrently fails to comply with its obligations stemming from this Regulation."

Art. 33 leaves it to the Member States to lay down rules on penalties applicable to infringements of the Data Act, thus leading to different standards within the Member States.[172] Additionally, the data protection authorities remain competent to impose administrative fines for the infringement of the GDPR.[173] Altogether this may lead to overlapping and parallel enforcement and thus to inefficient results and legal uncertainty.[174] This is partly addressed by the Council Presidency's proposal for a new para. 1a, proposing a list of non-exhaustive and indicative criteria for the imposition of penalties.[175]

Proposed Amendments:

– It should be considered how to ensure harmonised standards for penalties within the EU.

– Consider the interplay with the imposing of administrative fines under the GDPR.

---

[170] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 118.

[171] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 119.

[172] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 118.

[173] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 118.

[174] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 118.

[175] Council Presidency 2022/0047(COD) – 14019/22, p. 66.

4. Model Contractual Terms (Art. 34)

To assist parties in drafting and negotiating contracts with balanced contractual rights and obligations, the Commission should develop and recommend non-binding model contractual terms on data access and use and according to Rec. 83 "where necessary take into account the conditions in specific sectors and the existing practices with voluntary data sharing mechanisms."

Rec. 83 further explains:

> "These model contractual terms should be primarily a practical tool to help in particular smaller enterprises to conclude a contract. When used widely and integrally, these model contractual terms should also have the beneficial effect of influencing the design of contracts about access to and use of data and therefore lead more broadly towards fairer contractual relations when accessing and sharing data."

The model contractual terms are an important instrument for making the Data Act work effectively in practice.[176] Thus, *Leistner* and *Antoine* point to draft model contract terms for data sharing on contractual basis, on the necessary protection of trade secrets, the fairness test for B2B data sharing contracts and the minimum content for cloud service contracts defined in Art. 24.[177] At best, the model contract terms for data access, use, and sharing would already be provided with the Data Act becoming effective, to foster legal certainty.[178]

The LIBE Draft Opinion proposes to add, that as far as personal data are concerned, the Commission should consult the European Data Protection Board when developing such model contractual terms.[179]

The JURI Draft Opinion proposes, that these model contractual terms should also address the preservation of the confidentiality of trade secrets in accordance with this Regulation.[180]

The Council Presidency proposes to add non-binding standard contractual clauses for cloud computing contracts.[181]

With a similar aim of assisting parties in drafting and negotiating contracts with balanced contractual rights and obligations, the American Law Institute (ALI) and the European Law Institute (ELI) developed "Principles for a Data Economy", which could function as an example for model contractual terms.[182]

---

[176] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 119.

[177] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 119.

[178] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 119.

[179] LIBE PE737.389, p. 62.

[180] JURI PE736.696, p. 63.

[181] Council Presidency 2022/0047(COD) – 14019/22, p. 66.

[182] See https://europeanlawinstitute.eu/projects-publications/completed-projects/data-economy/.

XII. Final Provisions (Art. 36-42)

Chapter XI ('Final Provisions', Art. 36-42) allows inter alia the Commission to adopt delegated acts on monitoring switching charges and further specifying standards for interoperability and smart contracts. In case standards are insufficient, implementing acts are permissible under the Proposal.[183]

1. Amendments

In order to make use of the consumer protection cooperation network mechanism and to enable representative actions, Art. 36 and Art. 37 amend the Annexes to the Regulation (EU) 2017/2394[184] and Directive (EU) 2020/1828[185], as explained in Rec. 82.

2. Exercise of the Delegation

Art. 38(1) confers the power to adopt delegated acts on the Commission in accordance with Art. 290 TFEU for the previously discussed areas under Art. 25(4), 28(2) and 29(5), which are concisely summed up in Rec. 85:

> "a monitoring mechanism on switching charges imposed by data processing service providers on the market, to further specify the essential requirements for operators of data spaces and data processing service providers on interoperability and to publish the reference of open interoperability specifications and European standards for the interoperability of data processing services."

The Commission will assume said power at a time which is yet to be determined (see Art. 38(2)) and which hinges on the commencement of the Data Act.

When preparing a delegated act, experts designated by each member state as well as those from the European Parliament and of the Council are invited to relevant meetings of Commission expert groups, which is followed by a timely consultation of the member state-appointed experts on the draft of the delegated act in question (Art. 28(4); referring to the Interinstitutional Agreement on Better Law-Making of 13 April 2016, of which Sec. 28 and Sec. 3 of the Annex are pertinent). Upon adoption of the delegated act, the Commission is then to notify the European Parliament and the Council as per Art. 28(5) so that these institutions may object to the piece of legislation in question within three months (Art. 28(6) and Art. 290(2)(b) TFEU).

Ultimately, either the European Parliament or the Council can revoke the delegated power conferred upon the Commission, albeit with no retroactive effect on delegated acts which are already in force (Art. 28(3) and Art. 290(2)(a) TFEU.

3. Committee Procedure (Art. 39)

According to Rec. 86 implementing powers should be conferred on the Commission to ensure uniform conditions for the implementation of this Regulation. The Commission should

---

[183] COM(2022) 68 final (n 1) Explanatory Memorandum, p. 16.

[184] Regulation (EU) 2017/2394 of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[185] Directive (EU) 2020/1828 of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers.

> "adopt common specifications to ensure the interoperability of common European data spaces and data sharing, the switching between data processing services, the interoperability of smart contracts as well as for technical means, such as application programming interfaces, for enabling transmission of data between parties including continuous or real-time and for core vocabularies of semantic interoperability, and to adopt common specifications for smart contracts".

Art. 39 states that the Commission should be assisted by a committee within the meaning of Regulation (EU) No 182/2011[186].

4. Other Union Legal Acts Governing Rights and Obligations on Data and Use (Art. 40)

The Data Act should not affect specific provisions of acts of the Union adopted in the field of data sharing between businesses, between businesses and consumers and between businesses and public sector bodies that were adopted prior to the date of the adoption of the Data Act.

According to Rec. 88 the Data Act should also not affect the application of the rules of competition, and in particular Art. 101 and 102 TFEU. The measures provided for in the Data Act should not be used to restrict competition in a manner contrary to the TFEU.

5. Evaluation and Review (Art. 41)

After two years of the application of the Data Act, the Commission should carry out an evaluation of the Act and submit a report on its main findings to the European Parliament and to the Council as well as to the European Economic and Social Committee. That evaluation shall assess, in particular: (a) other categories or types of data to be made accessible in order to verify whether the access, use and sharing rights provided for the IoT sector can serve as blueprint for other constellations[187]; (b) the exclusion of certain categories of enterprises as beneficiaries under Art. 5 in order to allow a re-evaluation of actual market failures in regard to horizontal data access[188]; (c) other situations to be deemed as exceptional needs for the purpose of Art. 15 in order to provide the flexibility to take into account new exceptional challenges which potentially arise in the upcoming years[189]; (d) changes in contractual practices of data processing service providers and whether this results in sufficient compliance with Art. 24; and (e) the diminution of charges imposed by data processing service providers for the switching process, in line with the gradual withdrawal of switching charges pursuant to Art. 25.

Such an evaluation gives the legislator the chance to revise the Data Act in a rather short period of time in light of the very dynamic development of the regulated market sector.[190] It can also

---

[186] Regulation (EU) No 182/2011 of the European Parliament and of the Council laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers.

[187] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 122.

[188] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 122.

[189] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 122.

[190] Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 122.

be an opportunity to review whether the proposed access rights for public sector bodies are sufficient.[191]

The Commission should also, according to Rec. 87, evaluate the situation with regard to the relationship between the Data Act and the acts adopted prior to the date of adoption of the Data Act regulating data sharing, in order to assess the need for alignment of those specific provisions with the Data Act, to ensure consistency and the smooth functioning of the internal market.

The JURI Draft Opinion proposes an additional point (aa) to evaluate, whether the provisions related to trade secrets ensure respect for trade secrets while not hampering the access to and sharing of data.[192] JURI also proposes a new point (ea) concerning the evaluation of the application and functioning of Art. 27 on the international access and transfer of data.[193]

The ITRE Draft Report proposes a new point (ea) to evaluate the interaction between the Data Act and other relevant Union law to assess possible conflicting regulation, overregulation, or legislative gaps.[194] Indeed, including such an evaluation would further coherence in European data legislation.

The IMCO Draft Opinion proposes to add a new point (da) to evaluate the impact of the obligations provided for in Chapter VI, Art. 27 and Art. 29 on the cost of the cloud computing services in the EU, with a view to a full phase-out of switching fees.[195] The Council Presidency proposes a new point (f) to evaluate other products or categories of services to which access and use rights or the switching obligations could apply.[196]

6. Entry into Force and Application (Art. 42)

In order to allow the economic actors to adapt to the new rules laid out in the Data Act, they should apply from 12 months after the date entry into force of the Act, Art. 42 and Rec. 89. The IMCO Draft Opinion proposes to prolong this period between entry into force and application to 24 months.[197]

The Council Presidency proposes to add, that the obligation resulting from Art. 3(1) should apply to products and related services placed on the market after 12 months after the date of application of the Act.[198] It also proposes that the provisions of Chapter IV should apply to contracts concluded after the date of application of the Data Act.[199]

---

[191] Specht-Riemenschneider, L., *MMR* 2022, 809 (826).

[192] JURI PE736.696, p. 64.

[193] JURI PE736.696, p. 64.

[194] ITRE PE732.704, pp.58 et seq.

[195] IMCO PE736.701, p.53.

[196] Council Presidency 2022/0047(COD) – 14019/22, p. 69.

[197] IMCO PE736.701, p.53.

[198] Council Presidency 2022/0047(COD) – 14019/22, p. 70.

[199] Council Presidency 2022/0047(COD) – 14019/22, p. 70.

* * *