IX. Switching and Interoperability between Data Processing Services (Art. 23-31, Art. 33-35)

Chapter VI ('Switching Between Data Processing Services', Art. 23-31) imposes "surprisingly radical"[645] regulatory requirements of a contractual, (pre-)commercial, technical and organisational nature on providers of cloud, edge and other data processing services, to enable switching between such services. Having apparently been negotiated last[646], the provisions of Chapter VI have emerged from the institutional trilogue (in a characteristic display of legislative "hypertrophy"[647]) as substantially lengthened, with four new articles altogether.

Chapter VIII ('Interoperability', Art. 33-36) provides for essential requirements regarding interoperability for participants in data spaces and data processing service providers as well as for essential requirements concerning smart contracts. Further technological convergence is envisioned through the development of open interoperability specifications and harmonised standards for the interoperability of data processing services.[648] The rules contained in Chapter VIII have likewise been lengthened significantly as a result of the institutional trilogue.

With the exception of smart contracts addressed in Art. 36 (a "foreign subject"[649] primarily discussed in this work as an avenue for executing data sharing agreements on FRAND terms), both chapters are inextricably linked with one another. Domain name systems (DNS) offer a fitting illustration: within the realm of a data processing service, IP addresses of proximate servers are assigned to users accessing a website. This represents a standard capability of the cloud service model known as infrastructure-

645 Bomhard, D. / Merkle, M., *RDi* 2022, 168 (175).

646 After the trilogue meeting on 27 June 2023, an unofficial transcript of the inter-institutional agreement was leaked from which Chapter VI was still missing.

647 Veil, W., Auch der Data Act folgt dem Hypertrophie-Prinzip (Twitter, 20 July 2023) https://twitter.com/winfriedveil/status/1682070656580476928?t=digziO8W0DX0UgOJUH-6RA&s=19 accessed 18 September 2023 (observing that the final text of the Data Act has grown by almost 20,000 words compared to the original Commission proposal).

648 Commission, COM(2022) 68 final Explanatory Memorandum, p. 16.

649 Siglmüller, J., *MMR-Beil.* 2024, 112 (115).

as-a-service (IaaS).[650] For domain names to be organised as they were before the switching process, the DNS service used at the destination needs to map the new server infrastructure correctly and consistently. While this might constitute a relatively simple task, it is hard to accomplish unless the file storing the DNS configuration is exportable.[651] Switching operations beyond such basic syntactic and semantic data portability[652] are even less conceivable without technical standardisation in the way of interoperability – which is the subject-matter regulated by Art. 33 and Art. 35.

The Commission's Rationale for Taking Regulatory Action

In its Impact Assessment Report, the Commission observed 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*.[653]

The behavioural economic mechanics at play here merit further consideration. Typically, the value of a given cloud service is contingent upon the scale of its customer base. As a corollary, *network effects* – both direct and indirect – are bound to arise along with a significant agglomeration of customers. Particularly in software-as-a-service (SaaS) and platform-as-a-service (PaaS)[654] environments, customers will opt for a widely used platform that allows them to seamlessly exchange documents and applications with business partners.[655] Third-party developers will be drawn to the

650 Autorité de la concurrence, Avis 23-A-08 portant sur le fonctionnement concurrentiel de l'informatique en nuage (cloud), 2023, para. 28.

651 E.g., see the workflow for Google Cloud, Migrate to Cloud DNS https://cloud.google.com/dns/docs/migrating?hl=en accessed 24 September 2023.

652 Cf. Art. 33(2)(b) and the associated definition given by ISO/IEC 19941:2017(en), para. 3.2.3 and 3.2.4.

653 Commission, Impact Assessment Report Accompanying the document Proposal for a [...] Data Act, SWD(2022) 34 final, pp. 19 et seq.; Danyeli, G. ‚Die große Freiheit über die Wolke? Die Regelungen des Data Act zum Wechsel von Cloud-Anbietern und zur Interoperabilität, in Heinze, C. (ed.), Daten, Plattformen und KI als Dreiklang unserer Zeit, DSRI, 2022, p. 428 (rightly adding legal switching costs incurred from conducting data protection compliant transfers of digital assets).

654 Mentioned in rec. 81, among other cloud service models like IaaS; cf. the trichotomy, by now classical, put forth by Mell, P. / Grance, T., The NIST Definition of Cloud Computing (NIST Special Publication 800-145), 2011, p. 2.

655 Schnurr, D., Switching and Interoperability Between Data Processing Services in the Proposed Data Act, CERRE Report, 2022, p. 8.

marketplaces with the most customers. Similarly, their employees are likely familiar with (or even certified professionally for[656]) the particularities of the underlying IT system at the expense of lesser-known cloud service providers.[657] These network effects are further amplified by the fact that the cloud ecosystems with the greatest uptake are vertically integrated across several markets: they are able to source data from a given service to offer another one in a more targeted way[658] and to bundle together complementary products.[659]

As illustrated by the figures for 2022 in the public IaaS market[660], the resulting *lock-in effects* materialise in a concentration of market shares (81.1%) between five conglomerates based in the United States and in China (i.e., the so-called "hyperscalers" Amazon, Microsoft, and Google plus Alibaba and Huawei[661]), presently foiling what the Commission imagines as "the next-generation of fully interoperable, energy efficient and competitive European cloud-to-edge based services"[662]. Due to unabated growth in what customers expend on enterprise cloud solutions offered by these hyperscalers (an amount which has more than tripled from 2017 to 2023[663]), lock-in scenarios will certainly remain a valid concern in the years to come. The requirements under Chapter VI are therefore regarded as a necessary and potent policy option to lower market entry barriers for

656 Autorité de la concurrence, Avis 23-A-08, 2023, para. 267.

657 Autoriteit Consument & Markt (ACM), Market Study Cloud Services, ACM/INT/440323, 2022, p. 48; cf. Gans, J. / Herve, M. / Masri, M. (2023) 19:3 *European Competition Journal* 522 (562) (describing this as sunk costs for staff training).

658 ACM, Market Study Cloud Services, 2022, p. 50 (pointing to Google feeding search results into their cloud-based offerings).

659 ACM, Market Study Cloud Services, 2022, p. 62 (invoking the example of Microsoft 365).

660 Gartner, Gartner Says Worldwide IaaS Public Cloud Services Revenue Grew 30% in 2022, Exceeding $100 Billion for the First Time, 18 July 2023 https://www.gartner.com/en/newsroom/press-releases/2023-07-18-gartner-says-worldwide-iaas-public-cloud-services-revenue-grew-30-percent-in-2022-exceeding-100-billion-for-the-first-time accessed 16 September 2023; for a review of similar numbers in 2021, cf. Danyeli, G., Die große Freiheit über die Wolke? Die Regelungen des Data Act zum Wechsel von Cloud-Anbietern und zur Interoperabilität, in Heinze, C. (ed.), Daten, Plattformen und KI als Dreiklang unserer Zeit, DSRI, 2022, p. 429.

661 Note that in the EU, the fourth and fifth spots are instead occupied, respectively, by IBM and Oracle (cf. ACM, Market Study Cloud Services, 2022, pp. 34 et seq).

662 Council, SWD(2022) 34 final, p. 51.

663 Gans, J. / Herve, M. / Masri, M. (2023) 19:3 *European Competition Journal* 522 (524 et seq. and 538).

(European) data processing services (rec. 78) and to ultimately achieve an innovative "multi-vendor cloud environment" (rec. 100).

Self-regulatory approaches, most notably the SWIPO Codes of Conduct[664] developed in accordance with Art. 6 Regulation (EU) 2018/1807, have so far been unused save for a few providers (cf. rec. 79).[665] Curiously, despite the marginal success of this self-regulatory regime in addressing vendor lock-in (cf. rec. 78 and rec. 90), Art. 6 Regulation (EU) 2018/1807 is not repealed, but according to Art. 1(7) will remain applicable as a voluntary complement to the mandatory provisions of Chapter VI.

On the subject of *technical barriers* to switching, 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.[666] Studies by market authorities have shown this lack to be especially prevalent in the PaaS and IaaS sub-sectors, owing to proprietary databases and unreleased application programming interfaces (APIs).[667] In reaction to the *status quo*, rec. 100 notes that where market dynamics towards harmonised technical specifications are absent, European standardisation bodies on the basis of Regulation (EU) 1025/2012 should intervene at the behest of the Commission.[668] Rec. 103 puts this into concrete terms for semantic interoperability.

1. Surveying the Range of Data Processing Services (Art. 2(8), Art. 31)

A first major point of analysis relates to who is bound by the various obligations stated in Art. 23-31. In spite of more popular labels such as "cloud computing services"[669] contemplated throughout the legislative de-

664 Now rolled into one by SWIPO, Converged Code of Conduct for Data Portability and Cloud Service Switching, 2023.

665 Commission, SWD(2022) 34 final, p. 20 (noting by way of contrast that industry leader AWS alone offers in excess of 200 data processing services); cf. https://swipo.eu/current-swipo-code-adherences accessed 23 September 2023.

666 Council, SWD(2022) 34 final, p. 22.

667 ACM, Market Study Cloud Services, 2022, p. 56; Autorité de la concurrence, Avis 23-A-08, 2023, para. 526 et seqq.

668 Note however that common specifications (based on market-driven open interoperability specifications) offer an alternative route that sticks to self-regulatory developments (cf. Art. 35(5)).

669 Advocated pre-trilogue by the European Parliament (IMCO PE736.701, pp. 23 et seq.).

liberations, the Data Act employs the umbrella term "data processing service". The two-fold reasoning behind this broad terminological choice was to factor in edge computing (i.e., utilising computational resources close to the customer instead of remote data centres[670]) and to capture the all-encompassing reach of cloud-based infrastructure across the digital economy. Crucially, the use of the term "data processing service" extends beyond the switching requirements of Chapter VI to the interoperability standards under Art. 35 (read in conjunction with Art. 30(3)) and to the restrictions on transfers of non-personal data under Art. 32. Conversely, "data processing services" are yet to appear in other pieces of EU data legislation. For instance, Art. 2(13) DMA still employs the conventional framing as "cloud computing services"[671], whereas rec. 28 DGA finds that cloud storage and data intermediation services will generally not intersect.[672]

The Definition Supplied in Art. 2(8)

According to Art. 2(8), 'data processing service' means a digital service enabling ubiquitous, and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature, provided to a customer, that can be rapidly provisioned and released with minimal management effort or service provider interaction. Rec. 80 spells out in detail what is meant by the IT jargon making up various elements of this definition (ubiquitous, shared pool, scalable, elastic, (highly) distributed).

Proceeding in order of mention, what makes a data processing service 'ubiquitous' is the mechanisms via which resources are accessed in a given network promoting the use of thin clients (e.g., web browsers) and thick clients (i.e., equipment with significant processing capacity such as hard

670 Hon, W.K. et al., Cloud Technology and Services, in Millard, C. (ed.), *Cloud Computing Law* 2nd edn, OUP 2021, p. 17; Godlovitch, I. / Kroon, P., Interoperability, switchability and portability: Implications for the cloud, WIK-Consult Report, 2022, p. 14.

671 Further on their role as core platform services, cf. Geradin, D. / Bania, K. / Katsifis, D. / Circiumaru, A., The regulation of cloud computing: Getting it right (SSRN pre-print) pp. 6 et seq.

672 Specht-Riemenschneider, L., in id. / Hennemann, M. (ed.), Data Governance Act: DGA, Nomos 2023, Art. 2 para. 70.

drives[673]) alike. As rec. 80 elucidates, the pool of computing resources supplied is 'shared' in the sense that they are provided to multiple users, whereas the processing is carried out separately for each user (multi-client platforms[674]). Because outwards scalability and elasticity of computing resources according to fluctuating demand are phenotypical properties of cloud computing overall[675], a plethora of service models will fall firmly within the definition under Art. 2(8). Rec. 81 explicitly affirms this not only for IaaS, PaaS, and SaaS offerings, but is mindful of the existence of more granular or hybrid service models besides and beyond these three categories (sometimes represented in the label XaaS[676]). Rec. 80 and rec. 83 corroborate the rather wide-ranging impetus by recognising virtual IT infrastructure, most notably virtual machines, as a relevant type of computing resource. The stipulation in the concluding sentences of rec. 80 that resources can be allocated either in a distributed or highly distributed manner again embodies the juxtaposition of cloud and edge computing. On the flip side, not every XaaS provider will necessarily qualify as a data processing service because the server infrastructure they supply to the customer could be non-scalable by design.[677]

Online content services (Art. 2(5) Portability Regulation (EU) 2017/1128) such as linear (i.e. scheduled) broadcasting or non-linear (i.e. on-demand) music and video streaming services[678] had – quite controversially[679] – been dispensed from complying with all Chapter VI switching requirements un-

673 Oxford English Dictionary, s.v. "fat client (*n.*)," December 2023, https://doi.org/10.1093/OED/1155432750.

674 Bomhard, D., Auswirkungen des Data Act auf die Geschäftsmodelle von Cloud-Anbietern, *MMR* 2024, 109 (110).

675 Mell, P. / Grance, T., The NIST Definition of Cloud Computing. 2011, p. 2.

676 Boehm, F., Herausforderungen von Cloud-Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, *ZEuP* 2016, 358 (363) (mentioning sub-categories like data-as-a-service and communication-as-a-service); Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 62 para. 169.

677 Siglmüller, J., *MMR-Beil.* 2024, 112 (114) (raising the consequential question whether scalability should be construed in technical terms or per the stipulations in the service agreement).

678 Engels, S. / Nordemann, J.B., The Portability Regulation (Regulation (EU) 2017/1128) – A Commentary on the Scope and Application, 9 (2018) *JIPITEC* 179 para 22.

679 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 62 para. 170; Geiregat, S., The Data Act: Start of a New Era for Data Ownership? (SSRN pre-print), 2022, pp. 30 et seq. at para. 31.

der pre-trilogue versions of the Data Act.[680] The final wording of Art. 2(8), which has dropped this passage, does not change the exclusion of online content services in effect. Namely, rec. 16 firmly states that "textual, audio, or audiovisual […] content itself, which is often covered by intellectual property rights, inter alia for use by an online service, should not be covered by [the Data Act]".

In Particular: Cloud Switching Invoked by Consumers

By implication, defining data processing services extensively attributes significance to cloud switching in business-to-consumer (b2c) settings, especially compared with earlier drafts of the Act.[681] As Art. 2(30) lays out in the definition of "customer", the contracting party opposite a provider of data processing services can be a natural *or* a legal person. Consumers – a term defined in Art. 2(23) and sparsely used throughout Chapter II – do not unequivocally shine through in the notion of natural persons as customers. The same (tacit inclusion) is true of data subjects as per Art. 4(1) GDPR, which, again, are only related to their potential role as users under Chapter II (Art. 1(5)). To accommodate either concept, "customer" should be understood neither as presupposing legal or natural persons acting in a professional capacity nor as requiring a (monetary) payment to the provider.[682] On the latter point, Art. 23(c) (complemented by rec. 78) explicitly holds that entities supplying free-tier offerings count in among the targeted source providers.

Not having been fully anticipated by the legislator, the profound ramifications of the contractual clauses required by Art. 25(2) on existing rights granted to consumers and data subjects are in need of closer analysis. How these clauses interact with the right to erasure under Art. 17 GDPR, to have one's personal data ported under Art. 20 GDPR, and to retrieve digital content other than personal data in accordance with Art. 16(4) Digital Content

680 E.g., Commission, COM(2022) 68 final, p. 39.

681 Cf. Danyeli, G., Die große Freiheit über die Wolke? Die Regelungen des Data Act zum Wechsel von Cloud-Anbietern und zur Interoperabilität, in Heinze, C. (ed.), Daten, Plattformen und KI als Dreiklang unserer Zeit, DSRI, 2022, p. 430.

682 Geiregat, S., The Data Act: Start of a New Era for Data Ownership? (SSRN preprint), 2022, p. 29 para. 29; for instance, the provision of personal data pursuant to Art. 3(1) of the Digital Content Directive would suffice as the customer's contractual performance.

Directive (EU) 2019/770 (DCD) shall be explored below at the appropriate junctures.[683]

The Role of Data Processing Services in Operationalising Access and Sharing Rights

Chapter II, the access and portability regime for IoT-related data, 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.[684] What is more, providers of IoT services are increasingly relying on edge computing, processing data more locally to achieve quicker response times from sensors and mitigate privacy concerns.[685] "[L]imited possibilities regarding the portability of data generated by products connected to the internet " (rec. 20) are therefore bound to persist unless these data sets are easily unlocked from the existing and migrated to a new cloud environment by way of switching.[686]

Exemptions for Custom-Built Services and Beta Versions (Art. 31)

The switching requirements apply irrespective of the size and financial power of a data processing service. A proposal inspired by the rule devised for data holders in Art. 7(1), moving to exempt micro and small enterprises, did not gain sufficient traction in the legislative process.[687] Rather than bringing into play fixed quantitative criteria, the statutory exemptions for data processing services have shifted towards a more flexible situational assessment pursuant to Art. 31 ('Specific regime for certain data processing services'). Underpinning said article is the regulatory impetus to ease the

683 On Art. 17 GDPR and Art. 16(4) DCD, cf. sub 5; Art. 20 GDPR is discussed sub 9.

684 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).

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

686 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 60 para. 164.

687 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.

compliance burden on data processing services if they are not (yet) generally available on the market.

Art. 31(2) fully exempts those data processing services that have been made available temporarily in a non-production version for testing and evaluating purposes. Early access and beta testing programmes, whether private or public (i.e. restricted to the customer base at the time of release or open to new customers), should benefit from this exemption. As testing in late-stage development can typically last up to six months[688] depending on the number of beta testers and the complexity of the software architecture involved, the phrase "for a limited period of time" in Art. 31(2) should be interpreted liberally (in monthly intervals). This view is encouraged by the equivalent privilege for connected products undergoing testing pursuant to Art. 5(2), which altogether lacks a timeframe. Whether a non-production version for testing and evaluation purposes has been supplied by the provider of data processing services is therefore likely to emerge as the decisive question in interpreting Art. 31(2). Trial versions of a fully developed service do not qualify for a couple of reasons, chiefly among which is the fact that they are intended to promote the version with the full range of functionality and thus do not have testing and evaluation as their assigned purpose.[689]

Art. 31(1) addresses a different situation where (i) the majority of the service's main features has been custom-built to accommodate the specific needs of an individual customer *or* where (ii) all components have been developed for the purposes of an individual customer. In both cases, the data processing service must fall short of being offered at broad commercial scale via the provider's service catalogue, which roughly equates to the service being placed on the market (see Art. 2(22) and Art. 5(2) for connected products). Services falling within these parameters will not be required to deliver functional equivalence with the destination service (Art. 23(d), Art. 30(1)), can continue to charge for switching contrary to Art. 29, and do not have to ensure compatibility with harmonised standards and common specifications for the interoperability of data processing services (Art. 30(3), Art. 35). Because compliance with some of the more

688 For want of empirical data on this (at least concerning the public cloud sector), see the figure given by Google, What are software testing phases and GA? https://support.google.com/a/answer/11202276?hl=en accessed 22 September 2023.

689 Note as well that the text adopted by the European Parliament (P9_TA(2023)0069, p. 94) still featured data processing services "that operate on a trial basis".

invasive switching-related obligations is hence lifted by Art. 31(1), this exemption should be highly relevant in practice.[690] Still, providers must have in place a contractual environment that is conducive to switching (Art. 25) and which, on the technical side, is enabled by mandatory open interfaces (Art. 30(2) as well as by data exports upon request by the customer (Art. 30(5)). No further categorisation is made amongst custom-built or tailored services, meaning that providers of IaaS offerings could invoke a literal reading of Art. 30(2) ("data processing services other than those referred to in paragraph 1") to dismiss the associated duties. Paradoxically, their exemption from the far-reaching obligation to achieve functional equivalence would then leave almost no technical duties to implement switching, effectively upending Art. 30 and its division between IaaS providers on the one hand and (functionally more elaborate) SaaS / PaaS businesses on the other hand.[691] As this is hardly what the legislator will have intended by introducing Art. 31(1)[692], one should set the provision right through purposive construction, emphasising that *all* providers are subject to *all residual* technical obligations (i.e. apart from those governed by Art. 30(1) and Art. 30(3)).

Looking at the first scenario, the classification of a service as partially exempt hinges on what makes it "custom-built" and what its "main features" are under the law. As to the former, the notion of a custom-built service lends itself to particular legal uncertainty because such a binary criterion is ill-equipped to decide the nature of a cloud-based solution developed in multiple stages and processes.[693] A useful distinction could be drawn between custom-built and standardised software which was created for a reasonably broad range of customers and for a host of like use cases, with identical copies being marketed as such.[694] Regarding the latter, the main features of a data processing service will vary substantially case-by-case and (subjectively) from customer to customer. At any rate, said main features are to be appreciated in isolation and not with a view to functional equivalence and what destination services offer; they can therefore neither

690 Bomhard, D., *MMR-Beil.* 2024, 109 (110).
691 For the role of IaaS under Art. 30(1), see the concluding sentence of rec. 86 .
692 Cf. the last sentence of rec. 98 (acknowledging that once marketed at broad commercial scale, providers will eventually become subject to Chapter VI in its entirety).
693 Ennis, S. / Evans, B., Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence (SSRN pre-print), 2023, p. 16.
694 Rebin, I., in Spickhoff, A (ed.), BeckOGK Produkthaftungsgesetz (C.H. Beck 2022) § 2 para. 55.

correspond to the "shared features" pursuant to Art. 2(37) nor (arguably) to which "same service type" (Art. 2(9)) binds together a group of data processing services. Since the *majority* of main features is at issue, an objective assessment could involve which features characteristically denote the service model (for SaaS, integrated applications[695] such as proprietary analytics tools, messaging clients and office suites come to mind).

The second scenario of Art. 31(1) appears remarkably similar to, if perhaps more narrow in scope ("*all* components") than the first scenario. With rec. 98 containing no guidance on the matter, one can do little more than surmise what sets one apart from the other. A viable explanation hones in on the phrase "developed for the purposes of the individual customer", which could signify that the data processing service has been created for them from scratch (as opposed to "custom-built", suggesting non-standard modifications to existing software components).

2. The Terminology of Customer Activation: Switching, On-Premises Transfers and Multi-Homing (Art. 25(3), Art. 34(1))

Despite what its uniform heading ("Switching between data processing services") might suggest, Chapter VI is not rooted in a single action of switching away from the customer's original provider (known as the *source provider*).[696] Customers are instead free to choose between four basic options, boiling down to which contractual relationship they intend to maintain with the source provider and if they want to instruct a new service provider (the so-called *destination provider*) with managing their data and digital assets:

(1) switching to the destination provider (Art. 23(c), Art. 25(2)(a), Art. 25(3)(a))
(2) transfer to on-premises infrastructure (Art. 23(c), Art. 25(2)(a), Art. 25(3)(b))
(3) erasure of the customer's exportable data and digital assets (Art. 25(2)(c)(ii), Art. 25(2)(h), Art. 25(3)(c))
(4) in-parallel use of data processing services (Art. 34(1))

695 Autorité de la concurrence, Avis 23-A-08, 2023, para. 24.
696 Bomhard, D., *MMR-Beil.* 2024, 109 (110) rightly points out that regrettably, neither the source nor the destination provider are defined within the Act.

Although Art. 25(3) seems to indicate that customers may exercise the first two options independently from one another ("one or more of the following actions", viz. switching and transfers to on-premises infrastructure *cumulatively*), this must be understood as being directed towards what the customer can request under Art. 25(3)(c). Namely, the erasure of applicable data sets is inherent to both switching and on-premises exports pursuant to Art. 25(2)(h).[697] A juxtaposition with the language used in Art. 25(2)(a) ("to switch to a data processing service [...] *or* to port [...] to an on-premise ICT infrastructure")[698] as well as in rec. 82 (" switch to a different service provided by a different provider of data processing services *or* move to an on-premises ICT infrastructure") reveals that providers are not actually encumbered with a dual obligation. As for the in-parallel use of multiple data processing services, the one-directional actions of switching and on-premises exports are logically incompatible with multi-homing.

Turning first to *switching* as the phenotypical scenario of exiting one data processing service to use another in its place, the statutory definition in Art. 2(34) reads as follows:

> "'switching' means the process involving a source provider of data processing services, a customer of a data processing service and, where relevant, a destination provider of data processing services, whereby the customer of a data processing service changes from using one data processing service to using another data processing service of the same service type, or other service, offered by a different provider of data processing services, or to an on-premises ICT infrastructure, including through extracting, transforming and uploading the data".

Rec. 85 explains these last-mentioned steps in the switching process (extraction, transformation, and uploading). Additionally, a clarification is made whereby switching does not need to involve a wholesale migration from one large-scale cloud environment, but can also consist in unbundling a particular service from the contract (say, moving from one natural language processing tool to the next[699]). The label "switching" does not come without a considerable degree of incoherent terminology. *Sensu stricto*, it denotes the process of migrating data sets to infrastructure controlled by the destin-

697 Erasure is already possible after the passage of the notice period, cf. Art. 25(2)(c)(ii).

698 On a previous draft, cf. Geiregat, S., The Data Act: Start of a New Era for Data Ownership? (SSRN pre-print), 2022, p. 34 para. 34.

699 See the list compiled by Autorité de la concurrence, Avis 23-A-08, 2023, para. 32.

ation provider (e.g., according to Art. 25(3)(a)). More broadly speaking, "switching" is in use as the umbrella term for the three relevant actions sketched above (e.g., in Art. 2(34)). Problematically, the term is also affixed (in Art. 25(3)(b) and rec. 93) to operations destined for an on-premises infrastructure, thereby conflating both customer actions unnecessarily.

It is more accurate to frame *on-premises exports* not as a subset of (essentially cross-platform) switching, but as a distinct possibility of repatriating cloud-based resources. By choosing the expression on-premises ICT infrastructure, the Data Act ostensibly subscribes to the idea of making available exportable data and digital assets via on-premises (*in situ*) portals operated by the source provider. This has been favoured by some economists, particularly for business customers, to overcome information asymmetries to their detriment since multi-dimensional information is rather presented in its full context instead of being packaged and exported *ex situ*.[700] Crucially, on-premises ICT infrastructure is given precisely the opposite meaning under the terms of Art. 2(33), defining it as "ICT infrastructure[701] and computing resources leased, rented or owned by the customer, located in its own data centre and operated by the customer or by a third-party". On-premises transfers are hence construed not as *in-situ* access rights, but as a legal interest to receive[702] data sets akin to Art. 20(1) GDPR (or, perhaps, Art. 16(4) of Directive (EU) 2019/770). Because on-premises infrastructure is housed in the customer's data centre, lock-in effects are perceived as minor in comparison to remote data processing, which is why the actions laid out in Art. 25(2) do not cover on-premises infrastructure as the source of a switching operation.[703]

Finally, pursuant to Art. 23(1), the Data Act's regulatory regime for cloud switching now recognises the in-parallel (i.e., simultaneous) use of several data processing services, a usage pattern otherwise known as *multi-homing*. Non-business customers will often choose to engage with more than one platform (e.g., for cloud storage) in order to have multiple access and

700 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.

701 "ICT infrastructure" does not appear to be a legal term of art, especially given that Regulation (EU) 2022/2554 (the Digital Operational Resilience Act) leaves the concept undefined, too.

702 Geiregat, S., The Data Act: Start of a New Era for Data Ownership? (SSRN preprint), 2022, p. 34 para. 34.

703 Criticised by Lagoni, J., *CR* 2024, 91 (95).

backup methods with respect to the relevant data stock.[704] In business contexts, more than 80%[705] of customers have been found to deploy a so-called multi-cloud strategy (mentioned as such in rec. 99), spreading their digital assets between differently operated, complementary cloud services. However, a multi-cloud strategy is by no means tantamount to multi-homing in the sense that two services of the *same* service type are in use for the *same* sets of data.[706] Since well-known technical barriers to switching take hold and hamper multi-homing, Art. 34(1), oddly positioned in Chapter VIII, seeks to provide redress to customers. Apart from functional equivalence and – evidently – the clauses relating to the termination of service and the erasure of data at the source, providers are obliged to enable multi-homing both from a contractual and a technical angle.

3. Guiding Principles and Legal Status of the Switching-related Rights and Duties

For all its detailed provisions, Chapter VI is built on two remarkably short rules guiding the switching process end-to-end and determining the duty-based contractual, commercial, and technical framework which is meant to incentivise switching operations by customers. As expressions of the settled principles of proportionality (Art. 24) and of good faith (Art. 27), these related rules mark the general boundaries of providers' obligations and of the corresponding legal entitlements that customers hold.

In light of these principles, the present section also explores the (semi-contractual) legal nature of the rights and obligations created by Art. 23 et seq., paying particular attention to the construct of portability rights.

Scope of the Technical Obligations (Art. 24)

Art. 24 provides that the responsibilities of providers of data processing services laid down in Art. 23, 25, 29, 30 and 34 shall apply only to the ser-

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

705 See the surveys cited by Gans, J. / Herve, M. / Masri, M. (2023) 19:3 *European Competition Journal* 522 (542 et seq.).

706 Autorité de la concurrence, Avis 23-A-08, 2023, para. 76.

vices, contracts or commercial practices provided by the source provider. This is a direct consequence of Chapter VI targeting the source provider exclusively[707] (and not the destination provider, the exception being Art. 27). In essence, the underpinning idea is one of establishing a proportional sphere of responsibility so as not to overburden the source provider: it would be unreasonable (and likely detrimental to innovation and consumer choice[708]) to have the source provider recreate the contractual, commercial, and technical environment to the extent that all service features and contractual clauses of the destination provider can be linked to counterparts at the source.

Even more so, replicating (unknown or unique) functionalities of the destination service would be quasi-impossible without the source provider having some measure of access to the infrastructure of the destination provider[709], thus potentially compromising trade secrets. It is imperative to highlight that this concern was first raised with the objective of stifling the obligation of *functional equivalence* (Art. 2(37), 23(d), 30(1)).[710] While unsuccessful, the criticism impacted the position of the European Parliament[711] and of the Council[712], which ultimately prevailed in the form of rec. 86:

> "Providers of data processing services can only be expected to facilitate functional equivalence for the features that both the source and destination data processing services offer independently."

Further to that end, Art. 30(6) makes it plain that (source) providers are not required to develop new technologies or services in response to a request to switch or transfer made under Art. 25(2)(a), let alone proactively.

---

707 Cf. Bomhard, D., *MMR-Beil.* 2024, 109 (110); Geradin, D. / Bania, K. / Katsifis, D. / Circiumaru, A., The regulation of cloud computing: Getting it right (SSRN pre-print) p. 15 point out that other switching regimes under EU law such as Art. 106 of the Electronic Communications Code distributes the burden of compliance between the source and destination providers.

708 Ennis, S. / Evans, B., Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence (SSRN pre-print), 2023, p. 9 (fearing an incentive for firms to "dumb down" complex products).

709 Similarly, Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, CERRE Report, 2022, p. 17.

710 IMCO PE736.701, p. 3.

711 ITRE PE732.704, p. 44 ("shared core functionalities").

712 Council Presidency 2022/0047(COD) – 13342/22, p. 29 ("functionalities that both the originating and destination services offer").

The law therefore acknowledges the – far from unlikely – scenario that the destination provider offers functionalities which are absent from the service at the source (take certain applications and channels for team collaboration within an elaborate SaaS environment).

Against this backdrop, Art. 24 has generalised the rule that source providers are only liable to what pertains to their own service offering with the customer, and thus their sphere of influence.

Cooperation in Good Faith (Art. 27)

Art. 27 requires the parties (and in particular, the destination provider) to cooperate in good faith to make the switching process effective, enable the timely transfer of data, and maintain the continuity of the data processing service. Rec. 97 adds that data should be transferred securely in a commonly used, machine-readable format, and by means of open interfaces. For it not to pre-empt the more detailed modalities of data transfers under Art. 30, this latter regulatory commitment should be read to address destination providers transmitting necessary data to destination providers prior to switching.

The provision marks a logical continuation of Art. 24, reaching into the sphere of influence managed by the destination provider, and stands alone in targeting them. It remains to be seen in (judicial) practice, however, when a refusal to cooperate will be considered in bad faith and what consequences such a refusal would elicit. While Art. 27 means more than a mere encouragement to good-will cooperation, it hardly serves as a legal basis to compel destination providers to execute a technical action or specific business commitments.[713] By contrast, financial penalties pursuant to member state legislation made under Art. 40 or compensatory damages seem a more plausible prospect.[714]

On the opposite side of the switching process, source providers may likewise not obstruct its efficacy, for instance by mandating a single form or gateway for the customer to communicate their switching request.[715]

713 Bomhard, D., *MMR-Beil.* 2024, 109 (111 et seq.).
714 Bomhard, D., *MMR-Beil.* 2024, 109 (112).
715 Piltz, C. / Zwerschke, J., *CR* 2024, 153 (157).

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

The duty to remove obstacles to the "porting" of exportable data and other digital assets to a destination service or to on-premises infrastructure (Art. 23(c)) stands out as a firmly data-centric obligation. Were it not formulated *ex negativo*, this obligation could translate to a distinct right that customers may invoke against providers in broadly the same way as the right granted in Art. 5(1). Still, the nature of the underlying legal interest has stirred up some debate – a discussion which 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(c), jointly read with Art. 25(2)(a) and Art. 30, the creation of a statutory, i.e. "self-standing, immediately enforceable subjective right"[716]. The MPIIC proceeds on the assumption of a contractual right that entails both switching and portability obligations.[717] Relatedly, the Weizenbaum Institute derives from Art. 25(2)(a) a right to switch between providers, along with the conditions for exercising that right.[718] The members of CiTiP take a similar view, interpreting Art. 25(2)(a) in the sense of a "positive obligation to deliver on switching", which the co-legislators failed to frame as an explicit right to switch.[719]

While open to a wide margin of interpretation, caution is merited on what the obligations presented in Art. 23(c) and carved out in greater detail by Art. 25(2)(a) and Art. 30 truly amount to. Ultimately, the hypothesis of a self-standing "cloud portability right"[720] does not hold up to scrutiny. Art. 25(1) does not emulate the language of Art. 5(1), which is generally understood as a dedicated right to port IoT-related data bearing some

716 Geiregat, S., The Data Act: Start of a New Era for Data Ownership? (SSRN pre-print), 2022, p. 40 at para. 43; cf. also p. 29 at para. 28 (with regard to the original Commission Proposal); in apparent agreement: Ennis, S. / Evans, B., Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence (SSRN pre-print), 2023, p. 11 (noting an "extreme rebalancing of rights in cloud-based assets").

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

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

719 Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, p. 60.

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

resemblance to Art. 20(2) GDPR.[721] 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. 25(1) has to be related back to the overarching mandate under Art. 23(c) to remove all obstacles to porting – commercially, contractually, technically or otherwise. Accordingly, the source 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 course of switching under Art. 25(2)(a)(i).

The first-mentioned obligation, surfacing in Art. 23(c), lays the ground for uninhibited porting to take place and, from the perspective of the customer, could be regarded as part of a "right to switchability".[722] Critically, this was also how the Commission's Impact Assessment Report designated a policy option which prevailed over keeping the self-regulatory framework of Regulation (EU) 2018/1807.[723] Switchability, a concept underpinning Art. 23 on the whole, describes the ease – both in time and fees spent – by which customers can terminate a contract and rely on a workable technical framework in order to migrate their data and digital assets to a destination service.[724]

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[725] or, economically, as mandatory 'exit management'. Art. 25(2)(b) now consolidates this viewpoint by requiring the source provider to support the customer's exit strategy.

A duty to complete the switching process, which had formed part of the initial proposal[726], is presently not owed by the source provider unless, as

721 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, p. 28.

722 Commission, COM(2022) 68 final Explanatory Memorandum, p. 11.

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

724 Cf. Godlovitch, I. / Kroon, P., Interoperability, switchability and portability, WIK-Consult Report, 2022, p. 29.

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

726 Commission, COM(2022) 68 final, Art. 24(1)(a)(1) ("assist and, where technically feasible, complete the switching process").

rec. 85 puts it, "specific professional transition service has been obtained". Migration assistance to the customer and good faith-collaboration with the destination provider (Art. 27) aside, holding the source provider to the successful completion of the switching process has therefore become a matter for private ordering. The exception in this regard, reaching into the sphere of influence managed by the destination provider, is the duty under Art. 23(d) and Art. 30(1) (read with a view to the *caveat* under Art. 24) to facilitate that the highest possible degree of functional equivalence is achieved at the destination. On principle, however, the source provider is not liable to see the customer through the latter stages of the switching process. As rec. 85 elucidates, said responsibility is jointly borne by the destination provider and by the customer themselves:

> "Providers of data processing services and customers have different levels of responsibilities, depending on the steps of the process referred to. For instance, the source provider of data processing services is responsible for extracting the data to a machine-readable format, but *it is the customer and the destination provider who will upload the data to the new environment*, unless specific professional transition service has been obtained." (emphasis added)

Consistent with the plural form used in Art. 25(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 source provider:

(1) the right to demand a position at the source free from (pre-)commercial, technical, contractual, and organisational obstacles to 'switchability' (Art. 23)
(2) the right to have the source provider assist with the switching process, including through appropriate information and security measures (Art. 25(2)(a)(i), (iii), and (iv)), and to insist on good faith-collaboration with the parties involved (Art. 27)
(3) for data processing services of the IaaS variety[727], the right to obtain functional equivalence at the destination through the active contribution of the source provider (Art. 23(d), Art. 30(1))

727 See the final part of rec. 86.

Contrasted with the statutory right to (exportable) data portability found in Art. 30(5)[728], what these rights have in common is their origin within the contract. The concern that the source provider may conceivably take advantage of their bargaining position and alter its contents in a manner contrary to Art. 25(2) should therefore not be neglected.[729] For this provision especially, relying solely on public enforcement by the competent authority under Art. 37(1) falls short in remediating the switching-related obstacles faced by customers.[730] Calls for effective private enforcement in the court system are well-founded so that the conformity of a given contract with the requirements of Art. 25 can be adequately reviewed.[731]

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

Art. 23 merges the specific means and ends of regulation to ensure that customers can switch to one or more destination services (or conduct on-premises transfers). As to the enabling means of switching, providers of data processing services are obliged to positively implement the measures fleshed out in the subsequent articles. Art. 23 itself unites beneficial outcomes or ends of a customer-friendly switching process under the overarching ideal of *switchability* (on this term, see the preceding section). Namely, to accomplish switchability, providers shall not impose (or, if they have done so in the past, remove) the following obstacles to effective switching.[732] The provision thereby aligns with Art. 6(6) DMA, with the latter obliging gatekeepers to refrain from restricting users' ability to switch to another platform or remove obstacles to that effect.[733]

728 Cf. below at 9.

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

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

731 Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 67 et seq. n. 183 et seq.; *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").

732 The wording at the start of the second sentence of Art. 23 ("In particular") does not seem to imply that the measures would have to go beyond what is prescribed in Art. 25 et seq.

733 Louven, S., 'DMA Art. 6', in BeckOK Informations- und Medienrecht (42nd edn, C.H. Beck 2023) para 89.

Firstly, customers should not be deprived of their ability to terminate the original service agreement with the source provider after the statutory notice period has elapsed and the switching process has been completed (Art. 23(a), Art. 25). Secondly, the freedom of contract, that is to conclude a new service agreement with the destination provider covering the same service type (Art. 23(b)) may not be curtailed. Both provisions have to be regarded as safeguards of the customer's private autonomy and as prohibitions on imposing dark patterns, e.g., in the way of hidden terms and conditions.[734] Thirdly, Art. 23(c) stipulates that existing barriers for customers to port their exportable data and digital assets must be removed, including where the customer has benefitted from a free-tier (i.e., non-paid) offering by the source provider. This component of the right to switchability is available to customers irrespective of whether they have elected (phenotypical) switching, multi-homing, or on-premises transfers.

Crucially, digital assets (the most important subset of which are applications) and exportable data are mutually exclusive concepts. Under the Commission's proposal, data and applications both formed part of the umbrella term digital assets[735], which drew criticism for disregarding the diverging needs for data portability or application portability across the spectrum of IaaS, SaaS, and PaaS business models.[736]

By "digital assets" (Art. 2(32)), elements in digital format are meant, including applications, for which the customer has the right of use, independently from the contractual relationship of the data processing service it [the customer] intends to switch from.[737] Rec. 83 brings some clarity which elements besides applications qualify as digital assets: meta-data related to the configuration of settings, security, and access and control rights management, and other elements such as virtual machines and containers fall under the notion of digital assets. Some confusion remains over the meaning of 'applications.' The term could be misconstrued to cover the whole service offered to the customer by a source provider.[738] To avoid ambiguity, 'applications' are best interpreted in terms of IT architecture, for instance as computer programs that the customer could use on the

734 Martini, M. / Kramme, I. / Kamke, A., *MMR* 2023, 399 (402).
735 Commission, COM(2022) 68 final, rec. 72 ("all its digital assets, including data").
736 Ennis, S. / Evans, B., Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence (SSRN pre-print), 2023, p. 9.
737 Taken from Council Presidency 2022/0047(COD) – 14019/22, p. 37.
738 Bitkom, 'Bitkom Position Paper EU Data Act Proposal', 19 April 2022, 2022, p. 10.

source provider's cloud infrastructure.[739] In any case, the peculiar choice of 'digital assets' – a term that has hitherto largely been endemic to debates on so-called 'digital inheritance'[740] – demonstrates that the rules for switching embrace data portability and application portability alike.[741]

According to Art. 2(38), "exportable data" mean input and output data, including metadata, directly or indirectly generated, or cogenerated, by the customer's use of the data processing service, excluding any data processing service provider's or third party's assets or data protected by intellectual property rights or constituting a trade secret. Rec. 82 goes on to exclude data related to the integrity and security of the service from being exportable. Art. 2(38) is prefaced by the limitation "for the purpose of [Art.] 23 to 31 and [Art.] 35", probably to avoid applying the definition to data sets not concerning data processing services.[742] The omission of Art. 34 is easily adjusted for because that provision, in turn, references Art. 23(c) (amongst other parts of Chapter VI).

The inclusion of co-generated data as exportable has been welcomed in order to prevent lock-in effects.[743] Co-generated data sets can conceivably involve the source or destination providers as well as third parties like other customers; else, the parallelism of granting both groups the same exception for IP rights and trade secrets is hard to explain. *Schnurr* emphasises that the burden of proof rests with the source provider.[744] In any case, it would contravene the spirit of Art. 23 if the source provider could invoke IP rights or trade secrets as an all-out obstruction of migrating to the destination service – namely where the excluded data sets are not clearly specified.[745]

Fourthly, Art. 23(d) highlights functional equivalence in the use of destination services covering the same service type as the final objective of the switching process. Heralded by some as "practically central" *en route*

739 Geiregat, S., The Data Act: Start of a New Era for Data Ownership? (SSRN preprint), 2022, p. 32 at para. 33.

740 Geiregat, S. The Data Act: Start of a New Era for Data Ownership? (SSRN preprint), 2022, p. 33 at para. 33 with further references.

741 Which is made plain in Art. 35(2).

742 Cf. Art. 1(2)(e): "any data and services processed by providers of data processing services".

743 Geiregat, S. The Data Act: Start of a New Era for Data Ownership? (SSRN preprint), 2022, p. 32 at para. 32; precisely to that effect, cf. ALI-ELI Principles for a Data Economy, Pr. 19(2)(e).

744 Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, CERRE Report, 2022, p. 15.

745 See below on Art. 25(2)(e)-(f).

to interoperable ecosystems and IT infrastructures between the source and destination providers[746], functional equivalence is *not* a binding condition that source providers have to actively ensure. This is made clear not least by the passage "in accordance with [Art.] 24", meaning that source providers will ultimately not be liable for the performance of a competitor service outside their sphere of influence. Furthermore, Art. 23(d) does not anticipate or reference Art. 30(1), which establishes further duties concerning functional equivalence.[747] Rec. 86 corroborates said important division:

> "This Regulation does not constitute an obligation to facilitate functional equivalence for providers of data processing services other than those offering services of the IaaS delivery model."

Other data processing services – mainly those of the SaaS and PaaS variety – will only have to comply with Art. 23(d) and may simply not impose obstacles to achieving functional equivalence (as opposed to actively facilitating it pursuant to Art. 30(1)).[748] As drawing the line between IaaS and PaaS has become "an increasingly challenging and artificial pursuit"[749] in practice, one should expect source providers to assert that the majority of their data processing services fall within the PaaS bracket.

Lastly, Art. 23(e) addresses obstacles to unbundling data processing services referred to in Art. 30(1) from other data processing services provided by the source provider. The action of unbundling is intended to separate out IaaS services from the source provider's offering on the whole, thereby overcoming the aforementioned issues with classifying the service model. A comparison with a similar provision in Art. 12(a) DGA suggests that unbundling entails a structural separation, and would not prohibit a continued economic unity between all service models (including IaaS).[750] Alas, structural separation could only succeed where – as Art. 23(e) puts it – this is "technically feasible" in the first place. Rec. 93 frames the viability of un-

746 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. 30(1).

747 Functional equivalence is therefore discussed in greater detail sub 8.

748 Oblivious to this distinction: Bomhard, D., *MMR-Beil.* 2024, 109 (110 et seq.).

749 Ennis, S. / Evans, B., Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence (SSRN pre-print), 2023, p. 6; cf. Autorité de la concurrence, Avis 23-A-08, 2023, para. 26.

750 v. Ditfurth, L. / Lienemann, G., The Data Governance Act: – Promoting or Restricting Data Intermediaries? (2022) 23 *Competition and Regulation in Network Industries* 270 (284).

bundling differently as "the absence of major and demonstrated technical obstacles" that prevent it. Interconnected and integrated cloud ecosystems with IaaS elements will typically not be built on a modular architecture, which could in itself amount to a major technical obstacle.[751]

5. Contractual Enablers of Switching (Art. 25)

Whereas Art. 23 requires *ex negativo* that providers of data processing services do away with certain obstacles to 'switchability', Art. 25(2) stipulates the minimum content (rights and corresponding obligations) arising from the contractual agreement between the customer and source provider when it comes to switching to the destination service or moving to on-premises infrastructure. Art. 25(3)-(5) refine these obligations with special regard to the notice and transition periods triggered upon switching.

Art. 25(2) lists a wealth of clauses which to include in the contract between customer and source provider on a mandatory basis. The clauses drastically improve upon the bargaining position of customers of cloud and edge computing services and should have lasting impact on designing terms and conditions for service agreements in the cloud sector.[752] Rec. 96 goes further and encourages relying on (non-binding) standard contractual clauses and other tools for compliance – once adopted before the compliance date of 12 September 2025 (cf. Art. 41) – to foster both legal certainty and trust in data processing services.

Levelling the playing field, smaller source providers will often honour the customer's rights under one service agreement while holding co-extensive rights under a different service agreement with another (upstream) data processing service. Rec. 91 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 regarding their own service offerings."

751 Ennis, S. / Evans, B., Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence (SSRN pre-print), 2023, p. 14.

752 Bomhard, D., *MMR-Beil.* 2024, 109 (111).

Form of the Service Agreement (Art. 25(1))

Per its opening paragraph, Art. 25 requires that a written contract is to be concluded with the customer in a way that allows them to store and reproduce the contract. Any agreement in electronic form with the customer should be sufficient to meet this requirement[753], provided that the agreement has been made available for download before they sign it. A useful point of comparison can be drawn from Art. 28(9) GDPR, according to which an agreement in electronic form qualifies as a contract concluded "in writing".[754]

30-day Transition Period and Other Time Frames

Taken as an ensemble, the clauses required by Art. 25(2)(a), Art. 25(2)(d), and Art. 25(2)(g) determine the general timeline for the switching process. Accordingly, the procedure consists of four major steps.

At the outset, the customer submits a *request* indicating their broad intention to switch, that is without necessarily specifying if they prefer cross-platform switching, erasure of their data and digital assets at the source, multi-homing, or on-premises transfers. The wording of Art. 25(3) ("may notify the provider of data processing services of its decision to perform one or more of the following actions upon termination of the maximum notice period") appears to grant the customer discretion over disclosing their choice, but in doing so remains strikingly vague. The final sentence of rec. 85 errs the other way, stating that customers "should inform" the source provider about their decision. Art. 25(3) therefore lends itself to (at least two) diametrically opposed readings: according to the first, the customer may *only* notify the source provider of their decision upon termination of the maximum notice period (Art. 25(2)(d)), which is indeed reflected in

753 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, pp. 39 et seq. at para. 41 (advocating for the phrase "durable medium"); moreover, cf. Piltz, C. / Zwerschke, J., *CR* 2024, 153 (156) (pointing to Sec. 126b German Civil Code).

754 Seegel, A., Cloud-Switching nach Data Act: Der Vorhang fällt, die Fragen offen!, CR-online.de Blog, 15 November 2023.

the syntax of the German-language version.[755] A second – more plausible – reading hones in on the source provider and suggests that they have to start the lengthy process of executing the requested customer action upon termination of the maximum notice period, *until* which point the customer may change their mind.[756]

The initial request is followed by the so-called *notice period,* which has to be specified in the contract. Under Art. 25(2)(d), the period shall not exceed two months, i.e., the customer at most has to give two months' notice. The maximum 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.[757] It is unclear if the maximum notice period is set in stone or whether it can be extended or otherwise modified by way of private ordering. Because the idea of an alternative (agreed upon) notice period fell through in the trilogue negotiations, one could argue that the two-months limit cannot be prolonged.[758] The answer lies somewhat hidden in rec. 89, holding that "[n]othing in this Regulation prevents [...] parties from agreeing on contracts for data processing services of a fixed duration, including proportionate early termination penalties to cover the early termination of such contracts". Hence, the notice period can be lengthened as a matter of private ordering.

Subject to possible extensions as per Art. 25(4)-(5), the ensuing *maximum mandatory transitional period* under Art. 25(2)(a) lasts 30 calendar days during which the service contract remains in operation. Providers can seek to extend the period prescribed to up to 7 months on the grounds of technical unfeasibility for a switching process to conclude within that time frame (Art. 25(3)). Broadly reminiscent of Art. 12(2) GDPR, due justification for the delay of the switching process must be given within 14 working days of making the switching request. Rec. 87 clarifies that the onus for circumstances constituting technical unfeasibility is fully on the

755 Unlike the English text, the sub-clause "wonach der Kunde den Anbieter von Datenverarbeitungsdiensten *nach Ablauf der maximalen Kündigungsfrist* gemäß Absatz 2 Buchstabe d über seine Entscheidung unterrichten kann" (emphasis added) removes any ambiguity, but is most likely the result of an error in translation.

756 This reading can draw upon Art. 25(2)(c)(ii), in which the end of the notice period coincides with the customer's declaration to erase exportable data and digital assets.

757 Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, CERRE Report, 2022, p. 14.

758 Cf. Ennis, S. / Evans, B., Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence (SSRN pre-print), 2023, p. 14.

source provider.[759] Capping the transition period at 7 months has drawn criticism for not being workable in more complex cases, e.g. when moving fully integrated enterprise IoT platforms.[760] Finally, a clause to extend the transition period for the purposes of the customer must also be included in the contract according to Art. 25(5) – an option which the customer may invoke prior to or during the transitional period in order to ensure the continuity of service (rec. 87).

After the transition period has elapsed, Art. 25(2)(g) mandates that a further 30 days (or more) be given to customers as the minimum *period for data retrieval.* During this time, the continued security of the relevant data must be ensured pursuant to Art. 25(2)(a)(iv), thus marking the end of the source provider's obligations in assisting with the switching process.

Exit Management through Comprehensive Information (Art. 25(2)(a)-(b))

Time frames aside, Art. 25(2)(a) goes on to establish detailed rules for source providers to offer various aspects of migration support to the customer; at the same time, Art. 25(2)(a)(ii) clarifies that they have to maintain business continuity under the contract. Essentially, source providers have to carry out a form of "exit management"[761] for their customers. Art. 25(2)(b) explicitly requires providers to support the customer's exit strategy relevant to the contracted services, including by providing all relevant information. Rec. 92 and rec. 95 flesh out the contents of the resulting to duty to inform: *inter alia,* customers have to be let in on the scope of the exportable data and digital assets, the intended procedures, tools and available machine-readable data formats involved, known technical restrictions, and the estimated time to complete the switching process. Further information is to be given on known risks to continuity in the provisions of the original service (Art. 25(2)(a)(iii)).

Importantly, Art.25(2)(a)(i) implies the possibility for customers to enlist the services of third parties in the switching process, to whom the source provider needs to furnish the above information as well. Apart from the fact

759 As proposed by Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, CERRE Report, 2022, p. 15.
760 ITRE PE732.704, p. 55.
761 Bomhard, D. / Merkle, M., *RDi* 2021, 168 (175).

that the customer may compensate these third parties, no further mention is made of their involvement.[762]

Effects on Termination of the Contract (Art. 25(2)(c))

Art. 25(2)(c)(i) deems the contract between the customer and the source provider terminated upon the successful completion of the switching process. Art. 25(2)(c)(ii) antedates the point of termination in case the customer merely wishes to have their exportable data and digital assets erased (i.e., without any switching intentions). The contract must contain a corresponding clause, along with a duty to notify the customer that termination has occurred. The notion of a "successfully completed switching process", is not detailed in either Art. 23(a) or Art. 25(2)(c)(i). This lack of conceptual clarity begs the question how "successful completion" is measured.[763] Rec. 92 underscores the successful, effective and secure nature of the switching process, which could point to an objective standard in the sense that the relevant exportable data and digital assets have been migrated to the destination service (as opposed to a perhaps more subjective effectiveness from the customer's point of view). Given the duty of notification, it appears that the source provider – and not the customer – should decide upon successful completion based on objective criteria.

The interplay of this termination *ipso iure* per Art. 25(2)(c) with statutory rights to terminate[764] the contract is entirely left unaddressed and is obfuscated by the wording of Art. 23(a): if the contract automatically ends by successfully completing the switching process, why do source providers have to remove obstacles against (ineffectual) termination thereafter?[765] A haphazard explanation would account for the edge case that customer and source provider have exceptionally agreed to revive the contract, perhaps

762 Cf. rec. 89, third sentence; *vice versa*, the first sentence of rec. 89 concerns the provider outsourcing parts of the switching operation to third parties.

763 Seegel, A., Cloud-Switching nach Data Act: Der Vorhang fällt, die Fragen offen!, CR-online.de Blog, 15 November 2023.

764 In Germany, under the prevailing – if over-simplifying – classification of SaaS arrangements as leases and PaaS / IaaS arrangements as service contracts (*Dienstverträge*), rights of termination are available under Sec. 543 and Sec. 626 German Civil Code, respectively (cf. Strittmatter, M., § 22 Cloud Computing in Auer-Reinsdorff, A. / Conrad, I. (ed.), Handbuch IT- und Datenschutzrecht, 3rd edn, C.H. Beck 2019, para. 31).

765 Seegel, A., Cloud-Switching nach Data Act: Der Vorhang fällt, die Fragen offen!, CR-online.de Blog, 15 November 2023.

because certain data sets were accidentally omitted during the retrieval period.

Art. 25(2)(c) creates further uncertainties regarding the effects of termination on the remuneration owed by the customer. Because termination is tied to the switching process, it is conceivable that the source provider could no longer demand compensation for its services once the transition period has started. Conversely, rec. 89 states that standard service fees do not constitute switching charges under Art. 2(36), pointing to a continuity of remuneration throughout the switching process.[766] Even so, the prospect of a long-term contract being terminated *ipso iure* is bound to impact the revenue recognition of cloud and edge computing businesses.[767]

Exportable Data and Digital Assets (Art. 25(2)(e)-(f))

The categories of data and digital assets which are subject to cross-platform switching or on-premises exports must be specified in a dedicated contractual clause (Art. 25(2)(e)). At a minimum, all exportable data pursuant to Art. 2(38) must be reflected in these data categories.[768] Read in conjunction with rec. 82, those categories must include the customer's input and output data, along with pertinent meta-data, that have been (co-)generated by the customer's use of the data processing service. Furthermore, the exclusion of particular data sets protected by intellectual property would have to be listed. As to the exclusion of trade secrets represented within the exportable data, Art. 25(2)(f) contains a distinct rule. Accordingly, the contract must identify which data categories are exempt from porting or on-premises transfers since they are specific to the internal functioning of the source provider's data processing service and their disclosure would pose the risk of a breach of trade secrets. Art. 25(2)(f) goes on to state that this exemption may not delay or impede the switching process.[769] Source providers may therefore not invoke the extension of the transition period under Art. 25(4) solely because trade secrets are affected; in other words, the effort needed to separate out the data sets concerned does not in itself constitute technical unfeasibility.

766 Extensively, Bomhard, D., *MMR-Beil.* 2024, 109 (111).
767 Id. and Bomhard, D./ Merkle, M. *RDi* 2022, 168 (175).
768 See above on Art. 23(c).
769 Taken from Council Presidency 2022/0047(COD) – 14019/22, p. 56.

Erasure of Data Held by the Source Provider after the Retrieval Period (Art. 25(2)(h))

Finally, the contract must guarantee full erasure of all exportable data and digital assets generated directly by the customer, or relating to the customer directly, after the expiry of the retrieval period (Art. 25(2(g)). Erasure can exceptionally occur *after* the window for data retrieval has drawn to a close if the customer and source provider have agreed to do so (e.g., after reviewing a complex and lengthy switching process). As Art. 25(2)(c)(ii) makes plain, erasure does not have to be linked to a switching request, but may be requested in isolation.

As a result, the scope of the data that are subject to erasure does not mirror the definition of exportable data and digital assets given in Art. 2(32) and Art. 2(38) respectively, instead limiting it to data generated directly by the customer or relating to them directly. Despite apparent intersections with the concept of personal data (Art. 4(1) GDPR: any information *relating* to an identified or identifiable natural person), Art. 25(2)(h) fails to take note of the fact that this contractual agreement on erasure will apply next to the data subject right under Art. 17 GDPR in applicable b2c cases.[770] However, such a complementary relationship can be deduced from rec. 94, stipulating that existing rights relating to the termination of contracts under the GDPR should not be affected. The data subject's right to erasure is hereby addressed given that the absence of a contract will remove the (future) basis for legitimate processing (Art. 17(1)(d), jointly read with Art. 6(1)(b) GDPR).[771]

Interplay with the Digital Content Directive

The contractual arrangements to be taken in accordance with Art. 25(2) are "[w]ithout prejudice to Directive (EU) 2019/770" (i.e. the DCD). Rec. 94 modifies this apodictic statement by maintaining that the Directive's rights relating to the termination of contracts "should not be affected". Another

770 For Chapter II rights, rec. 39 makes this clarification in unmistakable terms; generally, see Art. 1(5).

771 Paal, B.P., DS-GVO Art. 17 Recht auf Löschung ("Recht auf Vergessenwerden"), in id. / Pauly, D.A. (ed.), Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 3rd edn, C.H. Beck 2021, para. 26.

inclusive conflict rule is found in Art. 1(9), which encompasses the DCD[772] along with other pieces of legislation promoting consumer protection: the Data Act "complements and is without prejudice" to these laws. Crucially, data processing services have to be regarded as digital services within the meaning of Art. 2(2)(b) of the Directive.[773] A conflict therefore arises with the Data Act, at least on the subject of termination-related rights.

The uncertainties 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 DCD. In the view endorsed by the MPIIC, both laws should not apply in parallel. Because Art. 25 offers a greater level of interoperability and technological governance, it should exclusively apply to digital content, including in b2c relations, thereby pre-empting the directive as the less "ambitious" porting regime.[774] The members of CiTiP concur in the result that Art. 24 constitutes a *lex specialis* to the Directive, finding that Art. 11 et seq. DCD are not suitable for the intricacies of switching operations.[775] Conversely, *Geiregat* argues for dual application in the b2c sphere, with greater consumer protection in effect.[776] This stance deserves support, not least because violations of Art. 25(2) could thus be framed as lack of conformity with the subjective requirements of the contract (Art. 7 DCD).[777]

For example, the customer can elect to retrieve digital content other than personal data (Art. 16(4) DCD) from the source provider's infrastructure rather than conducting a (not dissimilar) on-premises transfer or initiating the cross-platform switching process. Again, as with the interplay between on-premises exports and switching *sensu stricto,* this should not duplicate the burden on the source provider. In the style of a *ius eligendi*[778], the in-parallel application of the Directive and the Data Act therefore stops where the customer has exercised one right over the other.

772 Schmidt-Kessel, M., *MMR-Beil.* 2024, 122 (125).
773 Rec. 19 of Directive (EU) 2019/770 (explicitly mentioning SaaS); cf. Schmidt-Kessel, M., *MMR* 2024, 122 (126).
774 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 65 n. 177.
775 Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, 62.
776 Geiregat, S. The Data Act: Start of a New Era for Data Ownership? (SSRN preprint), 2022, pp. 37 et seq. at para. 39.
777 Schmidt-Kessel, M., *MMR-Beil.* 2024, 122 (127).
778 Cf. Sec. 265 German Civil Code.

Private Enforcement?

Unlike the unfair terms regime established by Art. 13, the consequences of failing to include the contractual minimum as prescribed by Art. 25(2) are not mentioned by the legislator.[779] While the service agreement between customer and service provider would remain in operation, violations could lead to financial penalties (Art. 40) or could justify awarding compensatory damages to the customer.[780] With respect to private enforcement, one must differentiate between provisions that are directly enforceable (e.g., Art. 25(2)(d)) and those which require a close review of the stipulations made in the individual contract (e.g., the list under Art. 25(2)(e)-(f)).[781]

6. Transparency Obligations next to the Contract (Art. 26 and 28)

Notwithstanding Art. 23, one of the key (if somewhat implicit) conditions for an environment of switchability between data processing services is providing all relevant information to the customer in a clear manner. Various facets of this all-round duty to inform the customer manifest themselves throughout the switching process, namely with regard to exit management (Art. 25(2)(a)(iii), Art. 25(2)(b)), switching charges (Art. 29(4)-(6)), and multi-homing (Art. 31(3)).

Art. 26 expands upon the duty to inform in a discrete provision. It should mainly be understood as an annex to parts of Art. 25 in the sense that the relevant information cannot (or need not) be included in the original contract with the customer.

As for Art. 26(b), this auxiliary role *besides the contract* is accurate: accordingly, source providers have to refer the customer (via hyperlink, etc.) to a self-hosted up-to-date online register (e.g., a restricted website) with details of all data structures[782] and data formats as well as the relevant standards and open interoperability specifications in which the covered

779 *Contra* Piltz, C. / Zwerschke, J., *CR* 2024, 153 (156) (holding that the contractual clauses between source providers and (business) customers will be subject to unfair terms control under Art. 13).

780 Bomhard, D., *MMR-Beil.* 2024, 109 (111).

781 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 118 n. 330.

782 Cf. rec. 24 and Art. 33(1)(b); on this and related terminology, see below in the section on Art. 33.

data sets under Art. 25(2)(e) are available.[783] Art. 30(4) adds an obligation to update the register to reflect timely compliance with the standards that are currently in force.[784]

As for Art. 26(a), its content presents a significant overlap with the aforementioned Art. 25(2)(b), essentially re-stating what is listed in rec. 95. Because Art. 25(2)(b) requires that "all relevant information" should be provided, with rec. 95 elaborating on said information in the context of supporting the customer's exit strategy (i.e., precisely the subject matter of Art. 25(2)(b)), the repetition in Art. 26(a) has merely declaratory value.

In light of cloud computing resources being spread between data centres across the globe, most notably in the United States[785], the provision of data processing services carries a momentous international dimension. Art. 28 takes into consideration the prospect of international access and transfer of non-personal data[786] from an information and transparency point of view. Customers are to be informed via the source provider's websites, the URLs of which have to be listed in the service agreement pursuant to Art. 28(2).

First, according to Art. 28(1)(a), customers must be given notice which jurisdiction the physical ICT infrastructure (e.g., servers[787]) deployed for data processing of their individual services is subject to. In line with similar language introduced to the Data Governance Act, "jurisdiction" should be construed broadly enough to cover both EU member states and third countries[788], whilst accounting for jurisdictions in federal legal systems (e.g., in the United States).[789]

Second, Art. 28(1)(b) obliges source providers to make available a general description of the technical, organisational, and contractual measures ad-

783 Council Presidency 2022/0047(COD) – 14019/22, p. 57.

784 See below on Art. 30(3).

785 Taylor, P., Number of data centers worldwide 2023, by country (Statista, 17 September 2023) https://www.statista.com/statistics/1228433/data-centers-worldwide-by-country/.

786 With regard to personal data, Art. 13(1)(f) GDPR – potentially coupled with Art. 49(1) sent. 4 GDPR –- applies as the relevant notice obligation; cf. Paal, B.P. / Hennemann, M., in Paal, B.P. / Pauly, D.A. (ed.), Datenschutz-Grundverordnung. Bundesdatenschutzgesetz, 3rd edn, C.H. Beck 2021, Art. 13 DSGVO para. 19.

787 Cf. rec. 80.

788 Cf. Specht-Riemenschneider, L., in id. / Hennemann, M. (ed.), Data Governance Act, Nomos 2023, Art. 7 mn. 37 (deeming the wording of Art. 7(3)(d) DGA inconclusive on the matter of which jurisdictions are encompassed).

789 Hennemann, M. in Specht-Riemenschneider, L. / id. (ed.), Data Governance Act, Nomos 2023, Art. 21 mn. 83.

opted by them in order to prevent unlawful international governmental access to or governmental transfer of non-personal data held in the European Union. The provision has to be juxtaposed with Art. 32(1), which orders providers to adopt said measures, and could trigger a similar practice to exporting controllers under Art. 44 et seq. GDPR conducting transfer impact assessments.[790] Crucially, the information given only has to relate to the data held by the source provider[791] – and not to those (already) held by the customer or by the destination provider.

7. Commercial Enablers of Switching – Reduced Switching Charges (Art. 29)

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 source providers often charge significantly for the retrieval of data (so-called data transfer-out fees[792]) and for their onwards transfer (so-called transport fees[793]). Art. 29 aims to gradually put an end to these commercial obstacles. Relating back to Art. 23(b), the withdrawal of switching charges thereby fosters the ability for customers to conclude new contracts with destination providers.[794]

Key Concepts

According to Art. 2(36), switching charges are "charges, other than standard service fees or early termination penalties, imposed by a provider of data processing services on a customer for the actions mandated by this Regulation for switching to the system of a different provider or to on-premises ICT infrastructure, including data egress charges." Data egress charges, in turn, signify "data transfer fees charged to customers for extracting their data through the network from the ICT infrastructure of a provider of data processing services to the system of a different provider or to on-premises ICT infrastructure" (Art. 2(35)). The term therefore collectively addresses the aforementioned data transfer-out and transport fees.

790 With further references: Piltz, C. / Zwerschke, J., *CR* 2024, 153 (157).
791 Bomhard, D., *MMR-Beil.* 2024, 109 (111); cf. Art. 1(2)(f).
792 Gans, J. / Herve, M. / Masri, M. (2023) 19:3 *European Competition Journal* 522 (530).
793 Commission, Switching of Cloud Services Providers, 2018), pp. 42 et seqq.
794 Bomhard, D., *MMR-Beil.* 2024, 109 (110).

Rec. 89 reiterates that proportionate early termination fees can be agreed (in line with so-called "commitment models"[795]) and that standard service fees can be chargeduntil the contract with the source provider becomes inoperable. Crucially, additional services beyond the switching-related obligations of the source provider can still be performed at cost if the customer has agreed tothe price in advance (consider the specific professional transition service mentioned in rec. 85). In light of the wide range of such professional (transition) services as well as the standard service offering, it has been argued that the quantitative impact of removing switching charges remains limited.[796]

On the other hand, if the provider outsources certain tasks within the switching process to a third-party entity, rec. 89 demands that outsourcing remains cost-neutral to the customer. Finally – in the case of multi-homing – the source provider can only demand data egress charges to the extent that they have incurred such costs (Art. 34(2)).

The Timeline for Withdrawing Switching Charges (Art. 29(1)-(3))

For a period of three years starting on 11 January 2024 (cf. Art. 50), source providers may impose reduced charges compared to the amount they have previously billed their customers for switching to a new service (Art. 29(2)). As evidenced by Art. 29(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 (i.e., from 12 January 2027 onwards), switching charges shall be abolished altogether under Art. 29(1). During the legislative process, it was suggested (in vain) to further accelerate the total withdrawal of switching charges for consumers, eliminating them by the date on which the Data Act enters into force.[797]

Going in the opposite direction, some commentators have fiercely criticised the regime established in Art. 29(1)-(3). *Gans* and co-authors fear that the removal of data transfer-out costs in particular will materially shift the price structure to the effect that customers not intending to switch, trans-

795 Lagoni, J., *CR* 2024, 91 (94).
796 Id., at 93.
797 IMCO PE736.701, p. 41.

fer on-premises or multi-home will cross-subsidize customers that do.[798] *Leistner* and *Antoine* point out the financial burden linked to complex switching operations, calling into question the layered 'sunset period' for switching charges.[799] 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.[800] Following this line of reasoning, asymmetries in the financial capabilities of differently sized enterprises could have been remedied by allowing microenterprises and small enterprises (especially given their favourable treatment elsewhere in the Act[801]) to continue to claim reduced switching charges even after the sunset period under Art. 29(2) has elapsed.

Monitoring Mechanism (Art. 29(7))

In order to reach the targets set by Art. 29(1)-(3), the Commission may adopt delegated (i.e. tertiary) legislation to monitor the progress of diminishing switching charges during the 3-years transition period (Art. 29(7)). In other words, the Commission is empowered to verify if the respective deadlines under Art. 29(1) and Art. 29(2) have been met. Conversely, it does not follow that the Commission can object to any increase of switching charges within the cost-covering threshold of Art. 29(3) – as may be the case when accounting for inflation.

A delegated act adopted on the basis of Art. 29(7) must comply with the procedural requirements of Art. 45 and take into account the advice of the EDIB pursuant to Art. 42(c)(iii).

Pre-Contractual Notice Obligations (Art. 29(4)-(6))

Art. 29(4) imposes a pre-contractual obligation on providers of data processing services to supply customers with clear information on standard

798 Gans, J. / Herve, M. / Masri, M. (2023) 19:3 *European Competition Journal* 522 (528); with similar concerns on price setting: Bomhard, D., *MMR-Beil.* 2024, 109 (111).

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

800 Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, CERRE Report, 2022, p. 15.

801 Cf. Art. 7(1), Art. 15(2) and Art. 20.

service fees, early termination penalties, and reduced switching charges. Art. 25(2)(i) repeats this obligation as far as switching charges are concerned. Possibly because of their volatility, applicable switching charges have to be (re-)stated in a dedicated contractual clause.

Art. 29(5) obliges the provider to flag data processing services within their service offering that involve highly complex or costly switching or even make switching impossible without significant interference in the data, digital assets or service architecture.

In a similar vein to Art. 28, providers shall make the just-mentioned pieces of information available via a dedicated section of their website or in any other easily accessible way (Art. 29(6)).

8. Functional Equivalence across IaaS Environments (Art. 30(1))

Art. 30 strikes a key distinction within the vast range of data processing services. Some providers will supply scalable and elastic computing resources limited to infrastructural elements such as servers, networks and the virtual resources necessary for operating the infrastructure. On top of that, they do *not* provide access to the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements. These providers are subject to an enhanced switching-related obligation. Not only do they have to refrain from imposing obstacles to achieving functional equivalence (Art. 23(d)), but the providers of these services are bound by a much higher standard under Art. 30(1):

> "Providers [...] shall, in accordance with Article 27, take all reasonable measures in their power to facilitate that the customer, after switching to a service covering the same service type, achieves functional equivalence in the use of the destination data processing service."

In its final sentence, rec. 86 sheds light on the addressees of this obligation, revealing (*e contrario*) that Art. 30(1) targets providers offering services of the IaaS delivery model. As previously sketched, the resulting distinction between IaaS and PaaS (and, to a lesser degree, SaaS) is often hardly achievable.[802] For example, Identity and Access Management services (IAM) speak to this point because they are found across the PaaS / IaaS spec-

802 Ennis, S. / Evans, B., Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence (SSRN pre-print), 2023, p. 6 with further references.

trum.[803] Even if the lines were less blurred, Art. 30(1) can still be criticised for missing a clear justification to hold the providers of IaaS offerings to a tougher standard.[804] In search of a rationale, the observation that a given service within heterogeneous ecosystems of the PaaS or SaaS varieties will lack a clear equivalent or correspond to multiple counterpart services at the destination more often is not fully convincing (or indeed, alien to IaaS).[805]

Functional Equivalence – A Feasible Concept?

According to Art. 2(37) "functional equivalence" means "re-establishing on the basis of the customer's exportable data and digital assets, a minimum level of functionality in the environment of a new data processing service of the same service type after the switching process, where the destination data processing service delivers a materially comparable outcome in response to the same input for shared features supplied to the customer under the contract." The "same service type", in turn, signifies a set of data processing services that share the same primary objective, data processing service model and main functionalities (Art. 2(9)).

Rec. 81 clarifies that the conventional data processing models (IaaS, SaaS, PaaS, and so forth) are not necessarily coextensive with the operational characteristics defining a service type. As to these operational characteristics, the legislation remains silent: what constitutes the primary objective and main functionalities of a given service and, conversely, which functionalities are merely of ancillary or secondary importance to this primary objective? Whilst attempts to pinpoint the main functionalities of multipurpose business cloud platforms (e.g., AWS, Microsoft Azure, Salesforce or SAP S/4HANA) would have proven as futile[806], examples based on less complex service types such as cloud storage could have shed some light on what the same service type – and thus, functional equivalence – actually entails. Rec. 81 partly remedies this vagueness by opening up the notion "same service type" and accepting that data processing services "of the same service type may have different [...] characteristics such as performance, security, resilience, and quality of service".

803 Autorité de la concurrence, Avis 23-A-08, 2023, para. 32.
804 Ennis, S. / Evans, B., Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence (SSRN pre-print), 2023, p. 11.
805 Gans, J. / Herve, M. / Masri, M. (2023) 19:3 *European Competition Journal* 522 (559).
806 Cf. Siglmüller, J., *MMR-Beil.* 2024, 112 (115).

The definition of "functional equivalence" in Art. 2(37) is itself not immune to regulatory friction for it does not consider the interplay with a similar term defined in Art. 2(12) DCD:

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

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 Data Act.[807] If answered in the affirmative, specific contractual assurances on what the source provider may perform in terms of output could come into play.[808] While the Act 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(d) – would hardly require *preserving* each contractual arrangement on the main functionalities at the source.

The Best Effort to Achieving Functional Equivalence (Art. 30(1), Art. 30(6))

Source providers have to take all reasonable measures *within their power* to facilitate that the customer achieves functional equivalence post-switching. By making reference to Art. 27, the provision demonstrates that functional equivalence hinges upon the source provider's in cooperating with the destination provider *bona fide*. The emphasis on cooperation also marks a minor contrast to Art. 23(d) citing Art. 24, whereby efforts regarding functional equivalence are directly limited to the source provider's sphere of influence. Nonetheless, the principle of proportionality enshrined in Art. 24 holds sway over the cases governed by Art. 30(1) as well. For one thing, functional equivalence does not amount to duplication of service at the destination. For another, source providers are not required to develop new technologies and services in the name of functional equivalence according to Art. 30(6).[809] Rec. 92 confirms these observations:

> "A source provider of data processing services does not have access to or insights into the environment of the destination provider of data

807 Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, 63.
808 Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, 63.
809 Cf. Bomhard, D., *MMR-Beil.* 2024, 109 (110).

processing services. Functional equivalence should not be understood to oblige the source provider of data processing services to rebuild the service in question within the infrastructure of the destination provider of data processing services."[810]

The remaining part of Art. 30(6) states that source providers do not have to disclose or transfer (unlicensed) IP-protected digital assets or those containing trade secrets. This assertion is likely redundant since the customer could no longer claim the right of use for the respective digital assets in these cases anyway (cf. Art. 2(32)).

9. Interoperability Requirements Aimed at Data Processing Services other than IaaS (Art. 30(2)-(5), Art. 35)

Continuing the division along the lines of IaaS delivery models on the one hand, and PaaS / SaaS delivery models on the other, Art. 30(2)-Art. 30(5) turn to the latter. Coupled with Art. 35, intricate rules for the standardisation of data processing services are introduced, most of which revolve around the pivotal notion of interoperability.

Cloud Interoperability in a Nutshell (Art. 2(40), Art. 35(2))

As a concept, "interoperability" carries connotations of openness and interconnectedness, which is why it is generally thought to enhance innovation and consumer choice in data ecosystems.[811] In the realm of data processing services, linking them by way of interoperability could give rise to complex and diverse service ensembles.[812] Where the level of interoperability is high (bordering on over-standardisation), the concept can however exert precisely the opposite effects in negatively impacting security and reliability of service as well as innovation incentives on digital markets.[813] A balanced

810 Gans, J. / Herve, M. / Masri, M. (2023) 19:3 *European Competition Journal* 522 (558) attributes this recital to the European Parliament's mandate for negotiation.

811 Gasser, U., Interoperability in the Digital Ecosystem, 2015, pp. 9 et seq.

812 Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, CERRE Report, 2022, p. 12.

813 Gasser, U., Interoperability in the Digital Ecosystem, 2015, at pp. 14 et seq.; Godlovitch, I. / Kroon, P., Interoperability, switchability and portability, WIK-Consult Report, 2022, p. 26.

calibration of interoperability requirements and definitions is therefore needed.

According to Art. 2(40), interoperability means the ability of two or more data spaces or communication networks, systems, connected products, applications, data processing services or components to exchange and use data in order to perform their functions. This definition, which borrows from long-standing jargon in computer science[814] essentially applies to digital infrastructure *in toto*, addressing their ability to exchange data on multiple levels of abstraction. An interesting parallel can be drawn to Art. 2(29) DMA, which goes further by blending in certain aspects of functional equivalence ("[...]so that all elements of hardware or software work with other hardware and software and with users in all the ways in which they are intended to function"). Conversely, *Siglmüller* approximates interoperability under Art. 2(40) to "compatibility" as understood by Art. 2(10) DCD, describing the ability of digital content to function with hardware or software typically used for digital content of the same type, without the need for conversion.[815]

For the purposes of data processing services, the above definition is incomplete without looking at the specifics of cloud interoperability. Art. 35(2)(a) reproduces, to the letter, the five layers advanced by the International Standards Organization (ISO) as standards for cloud interoperability.[816] The first three layers relate to the ability of systems to communicate through common infrastructures (transport interoperability), data formats (syntactic interoperability), and data models (semantic interoperability). At the fourth layer, "behavioural interoperability" seems to describe a lesser form of functional equivalence by focusing on the result of the data exchange, which has to match the expected outcome (cf. Art. 35(1)(c)). Finally, the policy layer of interoperability essentially reflects compliance with legal and organisational frameworks.

Art. 35(2) goes on to codify the remaining components of the aforementioned ISO standard. Whereas (b) enumerates syntactic, semantic, and policy data portability, (c) turns to application portability with distinct

814 Cf. ISO-Norm ISO/IEC 19941:2017, Information technology — Cloud computing — Interoperability and portability (mentioned twice in rec. 90 and rec. 100); IEEE Standard Glossary of Software Engineering Terminology, 1990, p. 42.

815 Siglmüller, J., *MMR-Beil.* 2024, 112 (115).

816 ISO-Norm ISO/IEC 19941:2017, Information technology — Cloud computing — Interoperability and portability, pp. 36 et seq.

facets such as metadata portability. It remains unclear if this dual terminology mirrors the migration of exportable data and digital assets, of which applications form part pursuant to Art. 2(32). *Schnurr* points out the dependency of workable application portability and switching-related "service portability" on existing vertical interoperability between the service and the underlying platform infrastructure.[817]

Open Interfaces (Art. 30(2))

Data processing services not designated as IaaS (including edge computing services) need not cater for functional equivalence, but have to set up open interfaces, at no additional cost to customers or concerned destination providers (Art. 30(2)). Along with other avenues for access and communication such as websites or intranet portals, Application Programming Interfaces (APIs, the importance of which is singled out in Art. 33(1)(c)) qualify as open interfaces.[818] In recognition of APIs fundamentally contributing to (various levels of) cloud interoperability when made available, the second sentence of Art. 30(2) stipulates that the obligation to share APIs or open up other interfaces is designed and shall include sufficient information "for the purposes of data portability *and interoperability*".[819]

Under the approach put into effect by Art. 30(2), interfaces only have to be made available between the parties, i.e. not publicly.[820] More importantly, the defence not to disclose digital assets that are protected as intellec-

817 Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, CERRE Report, 2022, p. 12; for a different understanding of vertical interoperability (namely between upstream and downstream services), cf. Godlovitch, I. / Kroon, P., Interoperability, switchability and portability, WIK-Consult Report, 2022, p. 27.

818 Cf., e.g., Commission, Explanatory Notes on VAT e-commerce rules, September 2020, pp. 8 et seq.

819 First suggested by ACM, Proposal to enhance the draft Data Act: Based on a national market study into Cloud services, 2022 https://www.acm.nl/system/files/documents/proposal-to-enhance-the-draft-data-act.pdf;cf. Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, CERRE Report, 2022, pp. 18 et seq.;Ennis, S. / Evans, B., Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence (SSRN pre-print), 2023, p. 8.

820 By contrast, cf. the initial wording given by COM(2022) 68 final, p. 54 ("providers of data processing services shall make open interfaces publicly available and free of charge.").

tual property or as trade secrets as granted by Art. 30(6) will come into play. It therefore becomes a highly relevant question to which extent providers can claim copyright protection over or trade secrets represented in APIs. As to the former, while a majority of commentators dismisses the idea, the Court of Justice is yet to rule squarely on whether software copyright covers APIs.[821] As to the latter, APIs lend themselves to being protected as trade secrets (Art. 2(18)) owing to the underlying, potentially marketable source code.[822]

Even if invoked successfully, one could argue that the defence arising from Art. 30(6) cannot deprive the customer of the necessary technical means for switching. In other words, the general prohibition on imposing obstacles of a technical nature stated (Art. 23) implies that at least one viable open interface should be at hand.[823]

Standardisation En Route to Fully Fledged Interoperability (Art. 30(3), Art. 35)

Besides making available open interfaces, non-IaaS data processing services have to adhere to further regulatory standards. Art. 30(3) - extrapolated in Art. 35 - mandates that providers have to ensure compatibility with common specifications based on open interoperability specifications *or* with harmonised standards for interoperability. The relevant services have to be brought into compliance with these standards at least 12 months after the Commission has published references in a designated Union standards repository for the interoperability of data processing services (Art. 35(8)).

In stark contrast with Art. 33(5) and Art. 36(6), harmonised standards made by European standardisation organisations under Regulation (EU) No. 1012/2012 do not take precedence over common specifications adopted by the Commission.[824] Instead, the Commission enjoys discretion

821 Aplin, T. / Radauer, A. / Bader, M.A. / Searle, N., The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis, *IIC* 2023, 826 (850); concurringly, Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 46 (on interface specifications).

822 From a transnational perspective cf. Irion, K., 'Algorithms Off-limits', *FaccT '22,* 1561 (1566).

823 Cf. Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 66 n. 180.

824 Rec. 100 even points the other way: " [...] where market-driven processes have not demonstrated a capacity to establish common specifications or standards that facil-

over whether to initiate the drafting process for harmonised standards (Art. 35(4): "may request") and / or seize its own regulatory authority through common specifications (Art. 35(5): "may [...] adopt"). This has rightly been identified as an oversight on the part of the legislator for it may lead to conflicting interoperability requirements.[825] The undesirable prospect of two standardisation instruments covering the same subject-matter could be resolved, however, by understanding the Commission's discretion as a binary choice between harmonised standards and common specifications in practice. Said interpretation aligns with the limits on the Commission's regulatory power regarding common specifications, given that the views of member state authorities and other relevant expert groups and bodies need to be taken into account pursuant to Art. 35(6). In another deviation from the otherwise parallel regimes for data spaces (Art. 33(7)) and smart contracts (Art. 36(8)), the EDIB is not expressly mentioned here.

Crucially, common specifications adopted by the Commission are not a stand-alone regulatory instrument according to Art. 30(3), but find their basis in so-called *open interoperability specifications*. Art. 2(41) defines open interoperability specifications as technical specifications in the field of information and communication technologies which are performance oriented towards achieving interoperability between data processing services. Art. 35(3) adds that these specifications need to have been developed through an open-decision making process, thereby avoiding the prevalence of dominant firms' proprietary standards.[826] Also, they need to have gained market acceptance, among other procedural and substantive requirements laid down in Annex II of Regulation (EU) No. 1025/2012. Rec. 100 further sheds light on the self-regulatory origin of open interoperability specifications, noting that the Commission should rely "on parties in the market to develop relevant open interoperability specifications to keep up with the fast pace of technological development in this industry."

Irrespective of which standardisation instrument is chosen, the aforementioned layers of cloud interoperability as per Art. 35(2) ought to be adequately addressed. Other than interoperability, Art. 35(1) demands that the broader objectives in regulating data processing services (portability of

itate effective cloud interoperability at the PaaS and SaaS levels, the Commission should be able, on the basis of this Regulation and in accordance with Regulation (EU) No 1025/2012, to request European standardisation bodies to develop such standards […]".

825 Siglmüller, J., *MMR-Beil.* 2024, 112 (116).

826 Cf. Paal, B. / Fenik, M., *ZfDR* 2023, 249 (260).

digital assets, functional equivalence, security and integrity of service) must be taken into account as well. Lastly, Art. 35(1)(e) pays heed to technological neutrality and fast-paced evolution and innovation (cf. rec. 100).

Art. 30(5) – An Oblique Right to (Exportable) Data Portability

Should no relevant standards under Art. 30(3), read jointly with Art. 35(8), exist as of yet, Art. 30(5) contains a fall-back provision whereby all exportable data shall be exported in a structured, commonly used, and machine-readable format at the customer's request. This provision, which does not have an exact counterpart in Art. 4 et seq., responds to a problem frequently voiced during the consultation period, namely lacklustre standardisation in data formats.[827]

As with the access right under Art. 4(1), the mandate to use a "structured, commonly used, and machine-readable format" emulates the wording of Art. 20(1) GDPR.[828]

Unlike the switching-related rights bundled together in the contract with the source provider, Art. 30(5) codifies a discrete *statutory right to data portability* held by the customer. However, its inapplicability to IaaS offerings, exacerbated by the residual role as a fall-back provision for Art. 30(3), arguably limit the practical reach of the right considerably.[829] If deemed applicable, Art. 30(5) could transcend Art. 20(1) GDPR. While both provisions exclude inferred and derived data[830] and safeguard IP rights and trade secrets in similar ways[831], the notion of exportable data is broader in extending to non-personal data as well (cf. Art. 28(1)(b)).

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

828 On these format requirements, cf. sub V.2., above.

829 Cf. Schnurr, D., Switching and Interoperability between Data Processing Services in the Proposed Data Act, CERRE Report, 2022, p. 23 (advocating for Art. 30(5) to be elevated to the default requirement for all exportable data).

830 Cf. rec. 15 on the one hand ("[...]information inferred or derived from such data, which is the outcome of additional investments into assigning values or insights from the data, in particular by means of proprietary, complex algorithms, including those that are a part of proprietary software, should not be considered to fall within the scope of this Regulation [...]"; on the other hand, cf. Article 29 Working Party, 'Guidelines on the right to data portability' WP 242 rev.01, 5 April 2017, p. 10.

831 On the one hand, see Art. 2(38); on the other hand, cf. the settled interpretation of Art. 20(4) GDPR, e.g., by Brandt, E. / Grewe, M., 'Datenportabilität 2.0', *MMR* 2023, 928 (930).

Consequently, the question arises to which extent Art. 30(5) can operate next to (or is superseded by) the GDPR right to personal data portability where customers are data subjects, too. In order to give a sound answer, one must turn to Art. 1(5) which calibrates the interface of the Act's provisions with data protection law. In principle, both regulatory regimes are positioned in a complementary relationship, which the second sentence of Art. 1(5) explicitly affirms for the interplay of Art. 15, 20 GDPR with Chapter II's access and sharing rights. Where a conflict with data protection law presents itself, however, the rights enshrined in the GDPR are set to prevail.[832] A *conflict* in the established (technical) sense of the word goes beyond a simple disparity, and cannot be reconciled through a normative device that allows for the two colliding rules to co-exist.[833] For exportable data that prove to be personal data, given the switching-related notification and transition periods, the time frame under Art. 30(5) to respond to a porting request would typically exceed one month as per Art. 12(3) GDPR. To avoid having to separate personal and non-personal exportable data, that is to achieve a coherent data export despite the (perhaps unforeseen) conflict, the one-month period under Art. 12(3) GDPR could be integrated into Art. 30(5). At any rate, having the customer decide between a GDPR or a Data Act "route" to exporting their data hardly serves a practical demand.[834]

10. Interoperability Requirements within Data Spaces (Art. 33)

Data spaces are part and parcel of the European Data Strategy, with the "establishment of EU-wide common, interoperable data spaces in strategic sectors"[835] being regarded as a key priority for boosting data sharing in the public and private sectors. To date, although 14 of the so-called Common

832 Conducting a holistic analysis of Art. 1(5), Schmidt-Kessel, M., *MMR-Beil.* 2024, 122 (126) argues that the precedence of data protection law already follows from the "without prejudice" clause in the first sentence, thus regarding the conflict rule in the third sentence as "obsolete at best".

833 Specht-Riemenschneider, L., *ZEuP* 2023, 638 (647) (quoting authority, specifically Joined Cases C-54/17 and C-55/17 *Autorità Garante della Concorrenza e del Mercato v. Wind Tre SpA & Vodafone Italia SpA* at para. 60).

834 Steinrötter, B., *GRUR* 2023, 216 (223) (with respect to Art. 4 and Art. 5).

835 Commission, COM(2022) 66 final, p. 16.

European Data Spaces have been announced[836], none has been fully implemented. Presently, the Regulation on the European Health Data Space, a political agreement on which has been reached on 22 March 2024[837], appears to be the singular regulatory instrument underway. In part, this is due to the Commission choosing not to rely on "overly detailed, heavy-handed ex ante regulation"[838] in favour of agile tools such as regulatory sandboxes.

Crucially, Art. 33 is not necessarily concerned with sector-specific considerations, but sets out a high-level, i.e. sector-agnostic interoperability framework for all kinds of data spaces.[839]

Defining Data Spaces

In Art. 33(1) and rec. 103, the legislator restates 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" (emphasis added). The umbrella term "data spaces", however, continues to lack a legislative definition. Turning to the main policy documents on the matter, one can deduce at least that data spaces make up larger data ecosystems (and eventually, a single market for data[840]) as characteristically open infrastructures allowing for the pooling, access, and sharing of data sources.[841] Moreover, data sharing where one parti-

836 Common European Data Spaces are envisioned to serve the needs of the following sectors and policy areas: high-level environmental initiatives ("European Green Deal"), industrial manufacturing, healthcare, energy, mobility, financial services, research, agriculture, employable skills, media, cultural heritage, and the public administration; for an in-depth synopsis, cf. Commission, SWD(2022) 45 final, pp. 12 et seq.

837 Cf. the original proposal of the Commission, COM(2022) 197 final.

838 Commission, COM(2022) 66 final, p. 12; further on the Commission's agile governance approach, cf. Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, pp. 97 et seq.

839 As is noted by Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, p. 16.

840 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (76) (referring to Commission, COM(2022) 66 final, p. 6).

841 Bitkom, Data Spaces and Data Ecosystems - First Explainer and Current Status, 2022, p. 5 (citing Council, SWD(2022) 45 final, p. 2 and documentation on the GAIA-X project).

cipant in the infrastructure offers data or data services falls within the ambit of data spaces and, consequently, triggers the applicability of Art. 33.[842] Rec. 103 supports this finding in defining "participants" (formerly: operators[843]) in data spaces as entities facilitating or engaging in data sharing within common European data spaces, including data holders. Data spaces can accordingly be understood as forums for exchanging product and related services data as well.[844]

Art. 33 as an Overarching Rule Governing Data Processing Services?

Ushering in the standardisation regime of Chapter VIII, it has been posited that Art. 33 represents a *lex generalis* which governs data processing services as well. Consequently, Art. 35 would merely modify and build on the general interoperability requirements of Art. 33 by way of a *lex specialis*.[845] This supposition is mainly substantiated through the use of the label "data services" in Art. 33(1), which allegedly ties in with the narrower concept of data processing services.[846]

"Data services", however, does not unequivocally constitute the hypernym for data processing services. For one thing, rec. 113 plainly mentions both concepts without hinting at any terminological hierarchy between them.[847] Secondly, the term "data services" has hitherto solely been brought up in a policy context, with no clear technical (let alone statutory) meaning attributed to it.[848] Even if "data services" could be identified as a term of art with data processing services as its sub-set, Art. 33(1) and the rules of Chapter VI display too many incongruities to support a hierarchical (rather than separate) design of Art. 33 and Art. 35. To give an example, it is hard to square with a hierarchical understanding why the transparency obligation pursuant to Art. 26(b) stops at data structures and data formats when Art. 33(1)(b) further requires that vocabularies, classification

842 Extensively, Siglmüller, J., *MMR-Beil.* 2024, 112 (113).
843 Council Presidency 2022/0047(COD) – 14019/22, p. 38.
844 Take the mention of connected products in Art. 33(1)(c).
845 Siglmüller, J., *MMR-Beil.* 2024, 112 (113).
846 Id. at 113.
847 As is conceded by Siglmüller, J., *MMR-Beil.* 2024, 112 (112).
848 E.g. Commission, COM(2022) 66 final, p. 27 ("Roll out re-usable data-services on a large scale to assist in collecting, sharing, processing and analysing large volumes of data") or Gaia-X, Gaia-X Federation Services (GXFS)', 1 December 2021, p. 3 ("This is how new data services providing value to all participants will be created").

schemes, taxonomies, and code lists shall be described in a publicly available and consistent manner. Additionally, the vision of automatic access and transmission of data within data spaces, possibly continuously and in real-time, provide a clear indication that Art. 33(1)(c) is not intended to subvert the time frames for complex switching operations set out in Art. 25. Instead, connected products and data sharing agreements are mentioned, which fits more adequately into the data access and sharing ecosystem for IoT products and services that is germane to Chapters II and III of the Act.

Essential Requirements for Data Spaces (Art. 33(1)-(2))

Per its opening paragraph, Art. 33 enumerates, on a high level of abstraction, four categories of essential requirements to facilitate the interoperability of data, data sharing mechanisms, and services. The following paragraphs supply a variety of regulatory instruments (delegated acts, harmonised standards, common specifications, and guidelines) to flesh out the finer points of these essential requirements for a specific sector or for data spaces in general. These avenues for direct regulatory intervention have been interpreted as a consequential reaction to the limited success of the market-driven approach under Art. 20 GDPR to develop interoperable formats.[849]

According to Art. 33(1)(a), key properties of a given data set relating to its usability (content, use restrictions, licences, data collection methodology, data quality and uncertainty, i.e. likelihood of veracity[850]) shall be sufficiently described so that recipients can find, access, and use the data set. Where applicable, this information shall be given in a machine-readable[851] format. Art. 33(1)(b) mandates that formal aspects of the data set, most notably its format and structure as elaborated through relevant vocabularies, classification schemes and data taxonomies, shall be described in a publicly available and consistent manner. *Siglmüller* identifies (somewhat illogical) differences between the two norms as far as the modalities of disclosure are concerned. It would seem that the description per Art. 33(1)(b) need

849 Callewaert, C., Data Act und Datenportabilität - Lesson Learned?, in Heinze, C. (ed.), Daten, Plattformen und KI als Dreiklang unserer Zeit, DSRI, 2022, pp. 422 et seq.; cf. rec. 68 GDPR.

850 Butterfield, A. / Ngondi, G.E. / Kerr, A. (ed.), A Dictionary of Computer Science, s.v. "uncertainty", 7th edn, OUP 2016.

851 On the notion of machine readability, cf. sub V.2.

not be in a machine-readable format, and *vice versa,* the information under Art. 33(1)(a) could also be made available under the terms of a data licensing agreement.[852] Likewise, it does not stand to reason why Art. 33(1)(b) refrains from stating the usability of the data set for recipients as the intended regulatory goal, which – as in Art. 33(1)(a) – would imply a sufficient quantity of the information as well as the absence of data dumps.[853]

Art. 33(1)(c) highlights APIs as an imperative tool to access and transmit data automatically and, where technically feasible, do so continuously, in bulk download, or in real-time in a machine-readable format. Not least by referencing connected products at the end, the provision is clearly geared towards realising the user's right to access and share readily available data pursuant to Art. 4(1) and Art. 5(1), respectively. Again (as in the case of Art. 30(2)), the potential of awarding intellectual property rights over APIs needs to be accounted for.[854] This should however not thwart the mere description (i.e., documentation[855]) as required by Art. 33(1)(c).

Going beyond documentation, Art. 33(1)(d) stands out as the only genuine interoperability mandate for participants in data spaces.[856] Accordingly, participants have to provide the means to enable the interoperability of tools for automating the execution of data sharing agreements. Special emphasis is put on smart contracts, thus pointing to the requirements of Art. 36.[857]

Art. 33(2) acknowledges that the essential requirements under Art. 33(1) are, by their very nature, non-descript and in a state of constant flux due to technological and market developments. To remedy the inherent vagueness, the Commission is given the power to adopt delegated acts. These delegated acts must comply with the procedural requirements of Art. 45 and take into account the advice of the EDIB pursuant to Art. 42(c)(iii).

852 Siglmüller, J., *MMR-Beil.* 2024, 112 (113 et seq.).
853 A similar issue concerning the same piece of statutory language arises in the context of Art. 3(2)(a) and rec. 24 (cf. sub IV.3.).
854 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 82 n. 223.
855 Siglmüller, J., *MMR-Beil.* 2024, 112 (114).
856 Id. at 114.
857 Cf. sub VI. 7.

Harmonised Standards (Art. 33(3)-(4))

Adhering to Art. 33(4), the Commission shall request one or more of the three European standardisation organisations (CEN, Cenelec, and ETSI[858]) to draft harmonised standards on the matter of essential requirements for data spaces.

Art. 33(3) institutes a (non-rebuttable) presumption of conformity with the essential requirements prescribed by Art. 33(1) if a participant offering data or data services in the data space can show compliance with the relevant parts of the harmonised standards.

Common Specifications (Art. 33(5)-(10))

Where the Commission's request under Art. 33(4) has not been accepted by the European standardisation organisation in question, or where the harmonised standards are not delivered within the applicable deadline or within the parameters of the request, the Commission may intervene in the absence of harmonised standards published in the Official Journal and adopt common specifications (Art. 33(5)). Rec. 103 makes it clear that these common specifications rank lower than harmonised standards: they represent "an *exceptional fall-back solution* to facilitate compliance with the essential requirements of this Regulation, or when the standardisation process is blocked, or when there are delays in the establishment of appropriate harmonised standards" (emphasis added).[859]

The subsidiary power of the Commission is affirmed through the duties to notify a committee established under Art. 22 of Regulation (EU) No. 1025/2012 (Art. 33(6)) and to consider the advice of expert groups as well as consult with relevant stakeholders (Art. 33(7)). The obligations to review and, if necessary, amend common specifications upon the intervention of member states (Art. 33(10)) and to repeal common specifications where harmonised standards have been published (Art. 33(9)) further attest to this.

In parallel with Art. 33(3), Art. 33(8) raises a presumption of conformity if a participant offering data or data services in the data space can show compliance with the relevant parts of the common specifications.

858 Annex I of Regulation (EU) No. 1025/2012.

859 Cf. sub VI. 7. (regarding the parallel regime for smart contracts in Art. 36).

Guidelines (Art. 33(11))

Art. 33 concludes by affording the Commission the opportunity to adopt guidelines regarding the aforementioned (sectorial) common European data spaces. Importantly, Art. 30(h) DGA comes into play, according to which the guidelines are proposed to the Commission by the EDIB, specifically its third sub-group pursuant to Art. 29(2)(c) DGA.[860]

While the EDIB is accounted for here, the same cannot be said of the equally relevant Data Spaces Support Centre.[861]

860 Cf. Hennemann, M., in Specht-Riemenschneider, L. / id. (ed.), Data Governance Act: DGA, Nomos 2023, Art. 30 para. 28.

861 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 84 n. 232; cf. Council, SWD(2022) 45 final, p. 8.