ADRIEN ALBERINI
YANIV BENHAMOU

# DATA PORTABILITY AND INTEROPERABILITY

## An issue that needs to be anticipated in today's IT-driven world*

**When contracting for IT services, individuals and companies do not often think of the end the contractual relationship and, more specifically, of the retrieval of the data handed over to the service provider. Since the law does not provide for sufficient means to ensure data portability in such situations, it is advisable to anticipate this issue and contractually regulate how the data in question will be migrated at the end of the contractual relationship.**

### 1. INTRODUCTION

In today's hyper connected world, everyone with regular access to electronics and the internet hands their personal data over to third parties on a regular basis [1]. As consumers, this is most often the case when we use services provided by companies like Google (eg. Gmail) or Apple (eg. iTunes). But we also provide our data to third parties just by browsing the internet, visiting websites or using apps. In the corporate world, we rely on various IT solutions which are *increasingly cloud-based*. This means that the customer data is stored on the servers of the provider (or of a subcontractor of the provider) and provided to the user on a subscription basis. As a result of this evolution, from a technical standpoint, we tend to *lose control* over our data or the data of our customer. This is particularly the case when we entrust our data or the data of our customer to a third party without creating any back-up storage on personal servers or hard drives.

When the customer stops being satisfied with the services or no longer needs them, *data portability* (or data migration), i. e. the retrieval and transfer of the data to another IT provider, becomes of the utmost importance [2]. In legal terms, the *question* is then whether the customer has a *right to be provided* with his, her or its data and, should that be the case, *how* (in which format) and at *what price* the data must be returned at the end of the contractual relationship.

After addressing some public policy considerations relating to the right to portability (Section 2), we argue that the law does not currently provide sufficient means to data portability (Section 3). Therefore, individuals and companies whose data is processed by third parties would do well, in our view, to anticipate this issue and contractually regulate the migration of data at the end of their contractual relationships (Section 4). In our conclusion (Section 5), we summarize our position and briefly describe the potential consequences of legal uncertainty as to the migration of data.

### 2. ECONOMIC AND PUBLIC POLICY CONSIDERATIONS

**2.1 Preliminary observations.** The economic and public policy considerations regarding the creation of a right to data portability are relatively complex; essentially, they boil down to the dilemma addressed hereinafter, that shows that there is no clear economic justification underlying the introduction into the law of a right to data portability.

**2.2 Switching cost and lock-in issue.** The absence of data portability tends to *create lock-in situations,* i. e. situations in which it is difficult for the customer to switch to another IT provider. Indeed, most customers will have a *limited incentive to contract with a new IT provider* if they have to once again provide a full set of data (economically, such effort is referred to as switching costs). Lock-in situations are even more likely when a large amount of data has been provided (and further enriched by the IT provider) and the customer cannot be en-

ADRIEN ALBERINI,
PHD, GENEVA, LLM
STANFORD, PARTNER SIGMA
LEGAL, GENEVA,
ADRIEN.ALBERINI@
SIGMALEGAL.CH

YANIV BENHAMOU,
PHD, ATTORNEY AT LAW,
LECTURER UNIVERSITY
OF GENEVA, GENEVA,
YANIV.BENHAMOU@
UNIGE.CH

tirely sure that he/she has kept a complete copy of the data to be able to hand it over to the new IT provider without the assistance of the current one (in particular when the customer has entrusted all his or her data without any backup on his or her servers).

**2.3 Effort and cost issue.** As Swire/Lagos correctly put it: the right to data portability

"require[s] software and online service providers to create what we call an 'Export-Import Module', or software code that exports data seamlessly from the first service to the second service". [3]

Thus, the migration of data may, depending on the circumstances, require quite a *high volume of work and money* [4]. If the cost is imposed on IT providers, it amounts in effect to a barrier to entry that could have *an adverse effect on innovation and competition,* because smaller players may not be able to afford said cost [5].

*"When the customer stops being satisfied with the services or no longer needs them, data portability (or data migration), i. e. the retrieval and transfer of the data to another IT provider, becomes of the utmost importance."*

## 3. THE LAW: AN INSUFFICIENT MEANS TO RETRIEVE DATA

**3.1 Preliminary observations.** At the outset, it should be noted that most continental law systems do not provide for proper ownership to data corresponding to rights to tangible property. Similar rights may be provided in particular legal fields, such as IP rights, personality rights, rights on know-how based on unfair competition law or privacy rights, provided, however, the specific requirements of these particular fields are met. As a consequence, *no claim based on some sort of a general property rights* theory can be made to retrieve data from a third-party provider [6].

In the Sections that follow, we demonstrate that even if obligation law, competition law and data protection provide for a right to data portability, they also each have certain shortcomings in serving as a basis for that right.

**3.2 Uncertainty relating to the Swiss Code of Obligations.** The *Swiss Code of Obligations (CO)* [7] sets out a right to return anything received by the agent (Art. 400 par. 1 CO) which should, in our view, *be a basis for the right of the customer to request the migration* of his or her data, provided, however, that the contract in question qualifies as a *contract for services (contrat de mandat)* [8]. This latter condition is a major issue considering the diversity of IT contracts which may exist in practice. Although some IT contracts may qualify as contracts for services, most of them should rather be *sui generis* agreements comprising provisions typically stemming from contracts for work *(contrat d'entreprise),* thus excluding the application of Art. 400 par. 1 CO [9]. Needless to say, there is often uncertainty with regard to the qualification in each different situation [10]. Consequently, it is also often uncertain whether Art. 400 par. 1 CO would apply in a given case.

That being said and assuming Art. 400 par. 1 CO would apply, this provision should, in our view and as indicated above, provide for the right of the customer to request the migration of his or her data. Art. 400 par. 1 CO regulates the obligation of restitution by the service provider. The principle underlying this obligation is that the service provider should not be able to enrich himself or herself except through his or her fees [11]. The service provider must therefore return all goods, debts, or other values he received or created in the scope of the contract [12]. Although this was not always the case, it is now undisputed that data, particularly personal data, may be valuable. Therefore, data should fall within the scope of Art. 400 par. 1 CO.

In our view, the *cost of data migration* cannot be charged on top of the price for the provision of the IT services [13]. Indeed, the price for the provision of the services must include all related obligations, including the obligation of restitution [14]. Therefore, the service provider cannot object to the restitution by saying that data retrieval is a service that was not provided for in the contract as a way to obtain an additional fee [15].

Since the process is not regulated, however, there is some *uncertainty* in this respect. The parties are free to choose the data's *delivery format;* there are no procedural rules imposed by law. The format of the data, however, ultimately depends on the type of service contract and on the principle of good faith [16]. The format used cannot render meaningless the right of the client to access his or her own data. The recovered data must therefore be *usable and readable by the customer* without having to purchase additional services from the provider [17].

With regard to potential objections, the service provider cannot assert the classic defenses, including contract retention rights (Art. 82 CO) [18], or retention rights based on the Swiss Civil Code (Art. 895 CC) [19].

*"In our view, the cost of data migration cannot be charged on top of the price for the provision of the IT services. Indeed, the price for the provision of the services must include all related obligations, including the obligation of restitution."*

**3.3 Limitation of Competition Law.** At the outset, it should be noted that a general data portability right cannot be derived from Swiss or EU competition law. That said, the refusal of certain providers to transfer data could constitute, *under specific circumstances, an abuse of dominant position* [20].

From a classical dominance perspective, data portability could be validly claimed when the dominant undertaking prevents the emergence of innovative competitors because customers are locked-in. Data may represent raw material for a variety of services, and access to this data a condition that is essential to entering or efficiently operating in a specific market. On this basis, it is sometimes argued that a powerful undertaking could maintain its *dominant position* in the market due to its possession of a large amount of information that is difficult to duplicate *(essential facility doctrine)* [21] and abuse this position by refusing to share that information and thus excluding competitors [22]. At this juncture, though, we are not aware of any case where this theory has been decisively applied to prevent an undertaking from further data collection (for instance as the result of a merger or acquisition) or from forcing another organization to share its data [23].

In our view, data portability could also be validly claimed in a case of *relative dependence,* namely the economic or technological dependence of one partner (e.g. an SME) on another [24], provided of course the elements of an abuse are met [25]. In essence, a customer that contracted with one provider can find itself tied to that provider and could then claim that there is an abuse of dominant position, particularly if the customer contracted for storage services or for data processing and the service provider refuses to return the data in a format that can be used by other providers or at a disproportionately high price for the customer.

As a final point on this issue, it is worth noting that *EU competition law* has paid significant *attention to the concept of interoperability*. In the *Microsoft case* for instance, the EU Commission ordered Microsoft to disclose, within 120 days, complete and accurate interface information which would allow rival vendors to interoperate with Windows, and to make that information available on reasonable terms [26]. Particularly noteworthy is the fact that the requisite *degree of interoperability* was a difficult and disputed issue [27], and that Microsoft has been subsequently fined for charging unreasonable prices for access to interface information [28].

**3.4 Limitations of (New) Data Protection Law.** The question of data portability is very often discussed in the context of data protection law. Interestingly, contrasting approaches have been chosen in the EU and in Switzerland.

In the EU, the new *Regulation 2016/679 (GDPR)* [29] explicitly establishes the *right of data portability,* thus taking a major step towards guaranteed retrieval of personal data and the suppression of lock-in situations [30]. This new right is regulated in Art. 20 Regulation 2016/679, which sets out the obligation of any service provider qualifying as a "controller" to guarantee, free of charge, the retrieval of the personal data *"in a structured, commonly used and machine-readable format and [the transmission of] those data to another controller without hindrance from the controller to which the personal data have been provided"*. Operators must therefore develop a system that allows them to examine their databases and extract pertinent information therefrom. In reality, this constitutes an extension of the information and access rights of the data subject [31].

*Three limits,* however, must be mentioned regarding this new right:

→ First, the right to portability under EU law is *limited to data concerning natural persons* and does not extend to data of legal persons. This constitutes a major limit to data portability in B2B relationships.

→ Second, the scope of the right to portability is strictly *limited to personal data,* namely to data concerning and directly provided by the data subject either actively (e.g. email address, user name or password) or passively (e.g. search history, traffic data or heart rate data). This excludes data which is inferred or derived by the service provider (typically data that is collected by the service provider and associated with the customer's account or the results of an algorithmic analysis of an individual's behavior) [32].

*"From a classical dominance perspective, data portability could be validly claimed when the dominant undertaking prevents the emergence of innovative competitors because customers are locked-in."*

→ Third, the *data subject is not entitled to decide the format* in which he or she will receive the data, although there is a requirement for the data to be returned *"in a structured, commonly used, machine-readable and interoperable format"*. One might wonder whether the data controller will have to provide the data in one or several interoperable formats and what the requested degree of interoperability will be in each case. Regarding this requirement of *"machine-readable and interoperable format"*, some relevant lessons may be learned from cases in competition law, such as the Microsoft case [33] and developments relating to standard-setting organizations [34]. Such analysis would however go beyond the scope of this paper.

In light of these limits, one might well doubt whether the new data portability law will be a success or a failure. But one thing is certain: courts will play a major role in interpreting this right and defining its proper scope, particularly with regard to the concepts mentioned in the last bullet point above.

In *Switzerland,* the portability question was discussed in the 2013 Report of the Federal Council regarding the legal framework governing social media [35] and, more recently, in the 2016 Explanatory Report of the Federal Justice Department regarding the Draft Bill of the Data Protection Act [36].

In light of the statement made by the Federal Council, as reported in the Explanatory Report, the right to portability should *not be introduced in Swiss law* in the coming years. Indeed, the Federal Council indicated the following:

"The Federal Council considers that this right aims to enable the concerned individuals to reuse their data in order to foster compe-

tition, rather than to protect their personality rights. Moreover, the implementation of such a right raises concerns insofar as it requires consultation among data processors and probably (at least implicitly) an agreement on IT solutions and standards to be used. The impact assessment of the regulation showed in addition that that introducing such a right may increase costs, particularly for companies with more than fifty employees, which would have to hire more people. The Federal Council will wait for the results of experience with the law in the EU before introducing the right to portability in Switzerland. It will further carry out its analysis in the context of the Swiss Digital Strategy." [37]

Notwithstanding this wait-and-see approach adopted by the Federal Council, the *right to portability as defined in the GDPR should be quite common in Switzerland,* considering both the fact that the GDPR will apply *extraterritorially* to companies

> *"The data should at least be transferred in a structured way so as to ensure interoperability with widely-used IT systems. Otherwise, it may be practically impossible for the customer to use the data after the end of the contractual relationship."*

located outside the EU but that process data of EU residents [38], and the fact that many Swiss companies are likely to observe the GDPR as best practice (in order to adopt a more "data protection-friendly" stance). In addition and as indicated in previous Sections, such right may be claimed, under specific circumstances, under *competition law and/or the right to receive* anything by the agent (Art. 400 par. 1 CO) [39].

## 4. THE CONTRACT: AN APPROPRIATE MEANS TO RETRIEVE DATA

**4.1 Preliminary observations.** As indicated above, the law is in many instances an insufficient means for customers to recover data from their IT provider. Put differently, a natural person, and a company even more so, may have a hard time when their data needs to be recovered in an acceptable format or to be migrated from the IT provider to a new provider.

As a result, it is highly *advisable to anticipate this issue in the formation of IT contracts.* Typically, data retrieval, portability and interoperability is dealt with in a set of clauses spread out in the contract. The main provisions are generally included in a Section called "Consequences of Termination" and these provisions should be read in connection with the Section specifically addressing "Data Protection" or "Data Management and Security". In the most sophisticated agreements, such as complex outsourcing agreements, a "Migration Plan" or "Exit Plan" is in principle provided for as an appendix. This document regulates precisely how the data transfer will be operated at the end of the contractual relationship.

The following Section includes a *check-list* of provisions that should *ideally appear in any IT contract* in order to ensure proper data portability.

### 4.2 Check-list

*4.2.1 Definition of data.* The definition of data may seem rather useless at first glance, but data can be contractually defined in multiple ways. "Personal Data", "Customer Data" or "Project Data" do not have the same meaning (and once the question is on the table, it is often quite hotly debated among the parties).

A broad definition would typically encompass information both provided by and relating to the customer (such as information about the customer provided by third-parties or gathered by the IT provider), as well as any information derived from such information (this is generally the definition of "Customer Data" or "Project Data").

Personal data, also referred to as personally identifiable information, would typically have a much narrower meaning, often corresponding to the definition provided for in the GDPR, i. e.

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". [40]

*4.2.2 Data ownership.* While it may sound redundant, the agreement should explicitly specify that the customer is the owner of the customer, project or personal data. The clause addressing this point may for instance read as follows: *"Customer possesses and retains all right, title, and interest in and to Customer Data, and [IT Provider]'s use and possession thereof is solely on Customer's behalf."* [41] This clause is important as it clarifies that ownership over customer, project or personal data is vested in the Customer and forces the parties to think about the rights to be granted to the IT provider in relation to such data. It also creates a solid footing upon which the portability right can be based [42].

*4.2.3 Data portability and addressee.* The agreement should include a general principle according to which, upon its expiration or termination, each party shall promptly return any property (including customer, project or personal data) belonging to the other party.

Regarding the addressee of the data, the IT provider typically agrees to hand over the data to the customer. In the absence of any specific provision, it is less certain that the IT provider will agree to the transfer to another provider, in particular if this process requires some cooperation among the providers. Therefore, this point should ideally be anticipated and regulated in the contract. It should thus be clear that the customer shall have the right to retrieve such data (often referred to as controller-data subject portability) or to have them transferred to a third-party provider (controller-controller portability).

*4.2.4 Format of the data.* Data is in principle stored and processed by the IT provider in its databases according to a specific format and structure. Therefore, one option is to hand over the data to the customer in accordance with this format and structure. Alternately, the parties may agree on a specific format and structure. In any event, the data should at least be transferred in a structured way so as to ensure interoperability with widely-used IT systems. Otherwise, it may be practically impossible for the customer to use the data after the end of the contractual relationship.

*"The question often arises as to the erasure of data and whether the IT provider should keep a copy of the transferred data during a defined period. To the extent possible, this issue should also be anticipated in the contract."*

*4.2.5 Timing and cost.* Depending on the circumstances, the transfer of data may be quite a complex and time-consuming process and the IT provider may have little incentive to proceed with the transfer considering that the relationship between the parties is ending anyway. The Parties should thus discuss this issue in advance and agree on an agenda.

Organizing and transferring data requires work to be performed on the IT supplier's side. Obviously, this work generates costs (generally calculated in man/day). In complex agreements requiring substantial work for the transfer of data, the migration occurs often at cost or the customer agrees to bear part of these costs. In principle, the IT provider should not make any profit on the migration activity.

*4.2.6 Subcontracting.* In case the IT provider passes on the data to one or several of its subcontractors, the data may end up being fragmented and it may be difficult to even identify who is holding what piece of data, making the retrieval of data at the end of the contractual relationship difficult in practice. For this reason, it may be worth setting out in the contract that no subcontracting will take place without the prior written approval of the customer or, at least, clarifying that the subcontractors shall be bound to the IT providers and the categories and types of data that will be processed by them [43].

*4.2.7 Related issues.* Without going into too much detail so as not to extend the discussion beyond the scope of this paper, it is worth adding that other issues are related in practice to the portability of data. For instance, the question often arises as to the erasure of data and whether the IT provider should keep a copy of the transferred data during a defined period. To the extent possible, this issue should also be anticipated in the contract.

Further, data portability raises specific issues in the event of bankruptcy of the IT provider (or its subcontractors), it being specified that the customer will face, in these circumstances, the difficulties of enforcement law [44]:

→ First, such enforcement law difficulties may not be circumvented by contractual arrangements, even if the contract provides certain mechanisms (e. g. notification duty of the IT service provider, audit report revealing a poor financial situation).

→ Secondly, enforcement law is governed by the territoriality principle and may lead to the application of several laws in international contexts (e. g. cloud computing with servers located in different jurisdictions, or in case of subcontracting in different jurisdictions) [45].

→ Thirdly, a delicate distinction between various categories of data (data qualifying as copyrighted works or personal data and raw data, i. e. any data regarding the company, statistic, financial data, etc.) has to be operated. Indeed, these categories of data will be subject to different enforcement mechanisms. Data qualifying for instance as copyrighted works or personal data may be claimed based on the so-called *action en revendication* of Art. 221 LP [46], while raw data may not be requested per se but only a monetary claim can be made corresponding to the value of the data in question (Art. 211 par. 1 and 252 ss LP).

Customers should anticipate these bankruptcy-related issues in the IT contracts. In addition to the ownership of data, the IT contract should provide for data storage in jurisdictions recognizing specific rights in case of bankruptcy (e. g. Luxembourg), the segregation of data with other customer's data, the transfer of data to a third-party agent in case of insolvency *(escrow agent)* and/or full anonymization of data [47].

## 5. CONCLUSION

When data is handed over to a third-party service provider, one of the key issues is knowing what happens at the end of the contractual relationship. Does the customer have a right to recover his, her or its data and to have them transferred to another provider? How and at what price must the data be returned at the end of a contract? We argue that the law does not provide a sufficient answer to these questions.

In practice, contracts rarely regulate this question; and when they do, they only lay out the principle of data retrieval without providing the method to be used to do it (in particular format, price, timeframe). This lack of detail can result in avoidable litigation, as the service provider could be tempted to demand substantial sums of money for the retrieval and transfer while the customer could be tempted to demand the services free of charge. Such challenging situations can be avoided by anticipating portability and interoperability issues and carefully drafting appropriate provisions in IT agreements. ■

**Notes:** *Adrien Alberini (PhD, Geneva; LLM, Stanford) is a partner at sigma legal. His practice focuses on technology law (in particular intellectual property, data protection and competition law) and on the formation and financing of startups . Link to the institutional website: http://sigmalegal.ch/sigma/adrien-alberini-en/. Yaniv Benhamou (PhD and lecturer at the University of Geneva) teaches, conducts research and publishes in the areas of Intellectual Property, E-Commerce and Entertainment Law. In addition to his academic activities, he is attorney-at-law in a Swiss law firm, where he advises and represents clients before courts with regard to Commercial Law, in particular to Intellectual Property, Technology, Media & Telecoms and Data Protection. Link to the institutional website: http://www.unige.ch/droit/collaborateur/cema/benhamou-yaniv.html. **1)** For a contribution dealing with many aspects of the transfer of digital goods, including data portability, see Y. Benhamou/L. Tran, Circulation des biens numériques: de la commercialisation à la portabilité, sic! 2016/11, 571. **2)** In EU Regulation 2016/679 (GDPR), data portability is defined as the right of the data subject to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller (par. 68 of the Recitals and Art. 20 GDPR). On this regulation, see below 3.4. **3)** P. Swire/Y. Lagos, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, 72 Maryland Law Review 335 (2013), also available at SSRN (posted: 9 Oct 2012; last revised: 28 Oct 2015). **4)** A. Diker Vanberg/M. B. Ünver, The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?, European Journal of Law and Technology, Vol 8, No 1, 2017. **5)** Swire/Lagos (n. 3), N 2.1.4. See also R. H. Weber/L. Chrobak, Rechtsinterdisziplinarität in der digitalen Datenwelt, Jusletter 4 avril 2016, N 43, further specifying that if the level of protection varies from one jurisdiction to another, it could favor competitors benefiting from these gaps to the detriment of customers, so that jurisdictions should coordinate their regulations with each other. **6)** Benhamou/Tran (n. 1), analyzing various legal bases possibly founding an ownership right to data, including the concepts of commons and of right to tangible property, and concluding that ownership right to data corresponds to a contractual claim. **7)** Loi fédérale complétant le Code civil suisse (Livre cinquième: droit des obligations) of March 30, 1911 (SR 220). **8)** For an analysis of the right to data migration based on Art. 400 par. 1 CO, see Benhamou/Tran (n. 1), 584. **9)** Benhamou/Tran (n. 1), 584, support that most sui generis agreements in the IT sector rely primarily on the rules of both contracts for services and contracts for work and note that a provision of the contract for work (Art. 365 par. 2 CO) might lead to an obligation similar to the one set out in Art. 400 par. 1 CO. **10)** On the difficult qualification of contracts in the IT field, see Judgment of Federal Tribunal of 26 August 2008, 4A.265/2008, par. 2.1.2; M. Jaccard/V. Robert, Les contrats informatiques, in: P. Pichonnaz/F. Werro (éd.), La pratique contractuelle: actualité et perspectives. Symposium en droit des contrats, Genève 2009, 95 ss. On the difficult qualification of contracts in general, see the recent decision of the Supreme Court, 13 December 216, 4A_251/2016, where parties with a banking relationship disputed the qualification of contract for services (Art. 394 ss CO) or simple partnership (Art. 530 ss CO), and thus the right to return based on Art. 400 par. 1 CO or art. 541 CO. **11)** Benhamou/Tran (n. 1), 584; J. Broquet, L'action en reddition de comptes et en restitution de l'art. 400 par. 1 CO, in: F. Bohnet (éd.), Quelques actions en exécution, Bâle 2011, N 7. **12)** On this obligation in general, see Broquet (n. 11), N 2 and N 18–19; On this obligation specifically in relation to IT contracts and digital data, see Benhamou/Tran (n. 1), 584. **13)** The costs of migration include the costs tied to the restitution itself which are packaged (e. g. stamp costs, price of USB sticks or hard disks) as well as the costs relating to services (e. g. to go search federal files, data extraction, making data readable on other systems). **14)** Broquet (n. 11), N 12. **15)** On this issue in general, W. Fellmann, Berner Kommentar VI/2/4, Berne 1992, CO 400 N 58; F. Werro, Commentaire romand CO I, 2ème éd., Bâle 2012, CO 400 N 6. On this issue specifically in relation to IT contracts and digital data, see Benhamou/Tran (n. 1), 585. **16)** ATF 122 IV 322, par. 3c and cited references, JdT 1998 IV 109; Broquet (n. 11), N 33; Benhamou/Tran (n. 1), 585. **17)** ATF 122 IV 322, par. 3c, JdT 1998 IV 109; Broquet (n. 11), N 34; E. Neuenschwander, Cloud Computing eine aktuelle Betrachtung, Jusletter 1 June 2015, N 27; W. Straub, Cloud Verträge – Regelungsbedarf und Vorgehensweise, PJA 2014, 922; On this issue specifically in relation to IT contracts and digital data, see Benhamou/Tran (n. 1), 587. **18)** This is due to the absence of an exchange agreement as referred to in Art. 82 CO between, on the one hand, the (supplementary) restitution obligation of the trustee and, on another hand, the (primary) obligation of the principal to pay the trustee fees. ATF 122 IV 322, JdT 1998 IV 109; Judgment of Federal Tribunal of 15 October 2007, 5A.367/2007; P. Tercier/P. G. Favre, Les contrats spéciaux, 4ème éd., Zurich 2009, N 5169. **19)** Code civil suisse of December 10, 1907 (SR 210). This defense is not applicable in a digital goods context because such retention rights only apply to tangible goods (Art. 896 par. 1 CO), which are unlikely to be successfully applied in a claim regarding digital goods. E. Philippin, Commentaire romand, Propriété intellectuelle, Bâle 2013, LDA 12 N 8; Benhamou/Tran (n. 1), 585 and cited references. **20)** In EU law, Art. 102 TFEU (Treaty on the Functioning of the European Union); under Swiss law, Art. 7 of the Swiss Cartel Act (Loi fédérale sur les cartels et autres restrictions à la concurrence of October 6, 1995; SR 251). **21)** On this doctrine, see for instance the decision of the Commission of 24 March 2004 (COMP/C-3/37.792 Microsoft; OJ 2007 L 32/23). **22)** Diker Vanberg/Ünver (n. 4). **23)** See however the decision of Comco of 14 December 2015, Zusammenschluss betreffend Schweizerische Radio- und Fernsehgesellschaft/Swisscom AG/Ringier AG, DPC/RPW 2016/1, p. 299, in particular par. 244. Regarding this case, see C. Bovet/A. Alberini, Recent Developments in Swiss competition law, RSDA 2017/1, 102, N 10. See also Diker Vanberg/Ünver (n. 4), N 4, referring to the EU Google investigation and the German Facebook case. **24)** On the concept of relative dependence, see E. Clerc/P. Këllezi, Commentaire romand LCart, 2ème éd., Bâle 2013, LCart 4 II N 252 et seq. As these authors point out, the concept of relative dependence does not exist as such in every jurisdiction; in EU competition law, it may at best be part of the analysis which is carried out in relation to classical dominance. **25)** Benhamou/Tran (n. 1), 587; Weber/Chrobak (n. 5), N 37. **26)** See in particular the summary of the case and remedies available at http://ec.europa.eu/competition/sectors/ICT/microsoft/investigation.html. **27)** N. Economides/I. Lianos, A Critical Appraisal of Remedies in the E.U. Microsoft Case, available at http://www.stern.nyu.edu/networks/Economides_Lianos_Critical_Appraisal_Microsoft_Remedies.pdf, 361. **28)** See the information provided by the EU Commission at http://europa.eu/rapid/press-release_IP-08-318_en.htm?locale=en. **29)** Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119/1), which will enter into force on 25 May 2018. **30)** To be noted that the introduction of this new right has been criticized on the ground that data portability issues are likely to emerge when a company holds market power and should therefore be tackled only under competition law. See for instance Swire/Lagos (n. 3). **31)** Art. 13 ss Regulation 2016/679. **32)** Benhamou/Tran (n. 1), 586; L. Urquhart/N. Sailaja/D. McAuley, Realising the Right to Data Portability for the Domestic Internet of Things, SSRN (posted: 18 March 2017; last revised: 31 May 2017), 2 et seq. **33)** See in particular n. 26 above. **34)** See for instance the Geneva Internet Disputes Resolution Policies Platform, Topic 3 (www.geneva-internet-disputes.ch). To be further noted that the work performed by some standard-setting organization is particularly relevant for the interoperability of data. See for instance the ITU Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities (www.itu.int/en/mediacentre/Pages/2017-PR13.aspx). **35)** Report of the Federal Council in response to the Postulat Amherd 11.3912 of 29 September 2011. Legal framework for social media, 9 October 2013, ch. 9, 83, showing users' dependence on online service providers and discussing a digital "data transfer right" for users from one online platform to another. Cited by J. DE WERRA, Perspective «Inside-Out». Défis du droit d'auteur dans un monde connecté, sic! 2014, 194, 205. **36)** Explanatory Report of the Federal Justice Department regarding the Draft Bill of the Data Protection Act, 21 December 2016, available at https://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vn-ber-f.pdf. **37)** Explanatory Report (n. 36), p. 22. To be noted that the only exception under Swiss law – which is very limited in scope – can be found in the LTC, which regulates the portability of telephone numbers: the LTC anchored the principle of portability to phone numbers, namely requiring telecommunications providers to permit their clients to keep their phone numbers even when they want to change providers. ComCom then established rules regarding the operating methods of this principle, creating an obligation to establish network agreements among providers and the technical and administrative methods for the delivery of numbers. Annex 1 of the ComCom Ruling (Technical and administrative directions concerning phone number portability between telecommunications services). **38)** On the extraterritorial application of GDPR, see Art. 3 Regulation 2016/679. **39)** See above 3.2 and 3.3. **40)** Art. 4 par. 1 Regulation 2016/679. **41)** D. W. Tollen, The Tech Contracts Handbook, Cloud Computing Agreements, Software Licenses, and Other IT Contracts for Lawyers and Businesspeople, Second Edition, American Bar Association, Section of Intellectual Property, 2015, 100. **42)** Benhamou/Tran (n. 1), 589. **43)** The prior written approval of the customer for any subcontracting is even a requirement under the Draft Bill of the Data Protection Act (Art. 7), and, in the banking and insurance sector, under the revised FINMA Outsourcing Circular (§ 40). **44)** For further details on this issue, see Benhamou/Tran (par. 1), 587. **45)** Neuenschwander (n. 17), N 22. **46)** Federal Act on Debt Enforcement and Bankruptcy/Loi fédérale sur la poursuite pour dettes et la faillite of April 11, 1889 (SR 281.1). **47)** Benhamou/Tran (n. 1), 589.