Implementation of Digital Data Erasure: An Interdisciplinary Perspective

Yann Conti/Yann Schoenenberger*

Contents

* Yann Conti is a Swiss qualified lawyer and PhD Candidate at the Civil Law Department of the University of Geneva (Switzerland). He currently works as a research assistant at the University of Zurich.

Yann Schoenenberger has an M.Sc. in Communication Systems from the École Polytechnique Fédérale de Lausanne (Switzerland). He currently works as a software engineer in research and development in the private sector.

This contribution is the authors' own independent initiative, and their opinion does not represent that of any institutions to which they may be affiliated. References have been taken into account until 31 July 2023. The authors are grateful to the Max Planck Institute for Innovation and Competition in Munich (Germany) where most of the legal research has been carried out. The authors are thankful to the Young Digital Law 2023 team for their valuable comments.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

I. Introduction

A. Scope

Data erasure is a key issue in the context of informational self-determination. In today's increasingly digital world, more and more aspects of our lives are being stored and managed in digital form. As the volume and complexity of digital data continue to grow alongside its value in the eyes of sometimes conflicting interests, it is essential that it is well managed and regulated to ensure its security and privacy.

Faced with a digital economy that is increasingly beyond their influence, legislators on the European continent are regularly updating data protection laws whose foundations are still very new, with the aim of reinforcing citizens' control over their data and thus their capacity for informational self-determination. One of the latest trends in this regard is the enactment or strengthening of the right to have their data deleted upon request.

However, such a task may be more challenging than it first appears. In order to create effective legislation pertaining to data erasure, it is essential to possess a technical understanding of the mechanisms underlying digital data. Current legal frameworks often implicitly presuppose that digital data operates analogously to paper documents. Thinking in terms of this analogy is naive, limited and can lead to ineffective legislation. Unlike paper files, digital data can be easily duplicated, transferred, and manipulated, making it considerably more challenging to regulate.

This contribution adopts an interdisciplinary perspective, combining legal analysis with technical insights that showcase the difficulties in enforcing certain legislations and reveal areas of inefficiencies. Against the trend towards approaching emerging technologies from a legal perspective, this contribution aims to consider the law from a technical viewpoint. To expand its relevance, a comparative approach is adopted, examining the legal landscape in both the European Union and Switzerland concerning the right to erasure and identifying key differences. Accordingly, this contribution adopts a somewhat hybrid structure, allowing legal and technical aspects to be considered cohesively.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

We start by looking at some definitions from the technical perspective as well as some domain-specific considerations as this gives us an overview of how things effectively are. With that in mind, we take a look at how the legislation in the European Union and in Switzerland handle data erasure while considering relevance and applicability. Focusing on both the General Data Protection Regulation ("GDPR") and the Swiss Data Protection Act ("SDPA"), we highlight how both laws conceptualize erasure and, consequently, how legal scholars, data protection authorities as well as case law apprehend its implementation. Regarding the GDPR, while we touch upon practices of different Member States, the interpretation of erasure in German law is of particular interest given its extensive doctrinal contribution.

We conclude by taking stock of the situation regarding digital law through the lens of the issue of data erasure and opening up the discussion and giving our opinion about how the approach to these legal questions could be improved moving forward.

B. Key Terminology

In any interdisciplinary work, it is of utmost importance to have a common understanding of terminology as different communities might use the same terms to slightly mean different things.[1] This is why, before delving into the legal analysis, we want to define a few terms that are going to be used throughout this contribution. These definitions rely themselves on other terms, but we consider an informal and non-technical understanding of them to be sufficient for our purposes.

We mean by *(digital) data*, information that is represented as a sequence of symbols. Typically, data will be held electronically in files and the symbols will be bits. Those files can be stored in a data medium (or storage device) or transmitted over a network. One can think of a digital picture taken with a phone camera as a typical example of digital data. The sequence of bits simply encodes which color each pixel of the picture should be. We call analog data, data that is not digital, like paper documents.

There is no technical distinction between *personal data* and digital data in general, but the distinction is key in relevant legislation. We mean by personal data any data related to a particular natural person. If we continue the example of the digital picture, if the picture is an x-ray of Alice's teeth, then that picture is Alice's personal data. On the other hand, a picture of the Moon in an article of a news website would not be considered personal data.

[1] For the legal definitions of data subject, controller and personal data, the reader can refer to Art. 4 GDPR and Art. 5 SDPA.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

Note that the boundary may be fuzzy between what constitutes personal data and what does not. Especially in the era of Big Data, as data is processed and computations are made on aggregated and anonymized sets of personal data, it is a legitimate question to ask whether a piece of data retains its personal nature.

The *data subject* is the person to which the data are related. In our previous example, the data subject is Alice. Here again, it is not a technical definition, but it is a key concept in the data protection legislations and very relevant to us.

The *data controller* is the entity that has the custody of particular data. In the case of Alice's x-ray, the data controller may be her dentist or the hospital where her medical record is held. In the case of her social media posts then the data controller is the company running the social media platform. This is again a concept that is crucial in the context of the data protection legislations but that has no meaning from a purely technical perspective.

The *data medium* or *data carrier*, also called storage device or storage medium, is the physical material on which data are represented. In our example, that may be the hard drive of the work computer of Alice's dentist.

We mean by *data erasure*, a method by which data are destroyed but the data medium is preserved. The aim of erasure is having the data inaccessible. We will call *ordinary deletion* the customary actions that any layperson knows and uses to delete computer files. We will see that ordinary deletion may not constitute data erasure.

C. Liminary Technical Considerations

As is argued in much of the rest of this work, there seems to be a strong bias across legal texts to consider and conceptualize digital data in ways similar to paper documents. The effects of this bias are subtle yet profound and may lead to ineffective legislation. This is why it is important to keep a few technical considerations, summarized in Fig. 1, in mind from the get-go.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

	Paper data	Digital data
Storage	Expensive	Cheap
Retrieval	Slow	Fast
Processing	Hard	Easy
Mechanisms (anonymization, encryption)	Basic	Elaborate
Copying	Hard	Easy
Transport	Hard	Easy
Destruction	Easy	Hard

Fig 1. Rough synthesis of key differences between digital and analog data.

First of all, it is much easier, in general, to access and retrieve digital data than information that has been written down on paper.[2] It is also trivial to copy. Replication of data is routinely done for the purposes of performance or backups. These copies are by and large just as easy to do across jurisdictions over networks.[3] When making a copy of digital data, there is no quality degradation or loss of information.[4] A digital copy is truly, mathematically, indistinguishable from the original.

This ease of copying and the boundless nature of digital data is well exemplified by the issue of piracy. Consider the massive scale at which copyrighted material is

[2] Viktor Mayer-Schönberger, 'Delete, The Virtue of Forgetting in the Digital Age' (Princeton: University Press, 2011), 52 ff.

[3] Herman T. Tavani, 'Informational Privacy: Concepts, Theories, and Controversies', in Kenneth E. Himma/Herman T. Tavani (eds), *The Handbook of Information and Computer Ethics* (Hoboken: John Wiley & Sons, 2008), 131, 140.

[4] Mayer-Schönberger, 'Delete', 60; Luke Tredinnick, 'Digital Information Culture: The individual and the society in the digital age' (Oxford: Chandos Publishing, 2006), 70.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

routinely shared across various networks, internationally and with easy to implement measures that can be used to effectively conceal such activity. This example shows how tricky it can be to deal with digital data, but delving deeper into the specific question of piracy is well out of scope.

Second, the cost of storing digital data is tiny compared to that of traditional, analog data[5]. Moreover, this gap has historically tended to widen. One result of this dynamic is that it is in some cases cheaper for data controllers to keep all of the data they have ever accrued, than have to make decisions about what to keep and what to delete.[6] Note that this observation holds even without considering other, sometimes strong, economic incentives such as the commercial opportunities stemming from the processing or sale of big data.

Third, we want to consider the nuanced ways in which digital data only can be processed. There are some circumstances under which encryption or anonymization may be considered equivalent to erasure. Most of these techniques are unique to the digital realm and when they are not, consider redaction of paper documents, the differences are so big that it is a saner default to not consider them analogous.

Finally, a particularly overlooked fact is that every interaction with digital data is done through the intermediary of a machine, typically a computer.[7] In the case of erasure, this matters, because it means that erasure is hard to prove. It is straightforward to witness the burning of a paper file, for example. One can actually verify that the content of the pages is vanishing as the paper burns. On the other hand, when digital data is erased, for example by issuing a few commands on a computer, how can an external observer verify that the commands that are supposed to be executed actually are ? There are ways to approach this issue, of course, but it is way more subtle than apparent at first.[8] Even in the case of physical erasure, how can one know for a fact that the physical device being melted, for example, is indeed the one storing the data that needs to be erased? Note that this question is raised merely to draw attention to the complex issue of verifiability, we do not aim to discuss potential solutions to them.

All this, taken together, means that one cannot think of digital data as similar to any technology that existed before. We would like the reader to ponder these properties

[5] Mayer-Schönberger, 'Delete', 62 ff; Tavani, 'Informational Privacy', 140.

[6] Mayer-Schönberger, 'Delete', 68.

[7] Mayer-Schönberger, 'Delete', 58 f.

[8] See for instance Manos Athanassoulis/Subhadeep Sarkar/Tarikul Islam Papon/Zichen Zhu/Dimitris Staratzis, 'Building Deletion-Compliant Data Systems' (2022) *Institute of Electrical and Electronics Engineers Data Engineering Bulletin* 21, 32.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

and the way they can be combined when considering the following analysis. As we will see, the analogy with paper, although an enticing mental framework eventually proves to be harmful.

II. General Data Protection Regulation

A. Right to Erasure

The GDPR was adopted on 24 May 2016 and has been in force since 25 May 2018.[9] It is designed in a technological-neutral way in order to prevent that the regulation be circumvented based on the means of personal data processing.[10] Therefore, it is applicable to the processing of personal data by automated means as well as to manual processing if the personal data are contained or are intended to be contained in a filing system.[11]

The GDPR's ancestor – the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive, "DPD") – already provided for a right to erasure which was recognized as part of the guarantees contained in the right of access (Art. 12 (c) DPD).[12]

One of the key features of the GDPR is the enacting a right to erasure in Art. 17 which is separate from the right of access (Art. 15 GDPR). This right is entitled "Right to erasure ('right to be forgotten')".[13] It can be exercised if one of the grounds of Art.

[9] Art. 99 GDPR.

[10] Recital 15 GDPR.

[11] Recital 15 GDPR.

[12] Art. 12 (c) DPD: "Member States shall guarantee every data subject the right to obtain from the controller as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data".

[13] This contribution only addresses the right to erasure *stricto sensu*. The question whether and to what extent the right to erasure ("*droit à l'effacement*") and the right to be forgotten ("*droit à l'oubli*") are distinct rights will not be addressed in this article (see Jef Ausloos, 'The Right to Erasure in EU Data Protection Law, From Individual Rights to Effective Protection' (Oxford: University Press, 2020), 93 and Michael Montavon, 'Cyberadministration et protection des données, Etude théorique et pratique de la transition numérique en Suisse du point de vue de l'Etat, des citoyen-ne-s et des autorités de contrôle' (Freiburg: Schulthess, 2021), 621 ff). Indeed, the right to be forgotten refers more to the question whether public information can be removed from the public sphere (see Art. 17 (2) GDPR) - and the weighing up of interests between the conflicting rights involved such as the right to freedom of expression - than to the actual erasure of data. For similar reasons, we will not address the issue of delisting. From a legal perspective, the latter has a narrower scope since it applies only to search

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

17 (1) (a)-(f) GDPR are fulfilled. Legal, scientific or public interests may override the right of the data subject to have its data erased in a way that allows the further retention of data by the controller.[14] For the sake of this contribution focusing on the implementation of erasure, we assume that the conditions for erasure are fulfilled and that no legal grounds or overriding interests are applicable.

B. Defining Erasure

1. Erasure as Reflected in the GDPR

The legal text does not define what erasure means.[15] To our knowledge, there is to date neither a decision on the European level on the notion nor a specific guideline of the European Data Protection Supervisor devoted specifically to detail the notion of erasure. By interpreting the GDPR, we can however draw some guidelines on what must be understood by erasure.

First, we can put the notion of erasure into perspective through the definition of personal data processing by the GDPR. Art. 4 (2) GDPR defines the processing of personal data as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration,

engines and is geographically limited (see Eugenia Politou/Efthimios Alepis/Constantinos Patsakis, 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions' (2018) *Journal of Cybersecurity* 1). Moreover, from a technical point of view, delisting does not constitute data erasure as defined for the purposes of this article, because in many cases, delisting is just as weak as ordinary deletion.

[14] Art. 17 (3) GDPR. Further retention remains possible when data are retained "for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims" (Recital 65 GDPR).

[15] Marian Alexander Arning, 'Art. 17 GDPR', in Flemming Moos/Jens Schefzig/Marian Alexander Arning (eds), *Praxishandbuch DSGVO* (Frankfurt am Main: Recht und Wirtschaft, 2021) para. 410; Dietmar Jahnel, 'Art. 17 GDPR', in Dietmar Jahnel/Christian Bergauer (eds), *Kommentar zum DSGVO* (Wien: Jan Sramek, 2021) para. 12; Alexander Dix, 'Art. 17 GDPR', in Spiros Simitis/Gerrit Hornung/Indra Spiecker (eds), *Datenschutzrecht, DS-GVO mit BDSG* (Baden-Baden: Nomos, 2019) para. 5; Wolfgang Däubler, 'Art. 17 GDPR', in Wolfgang Däubler/Peter Wedde/Thilo Weichert/Imke Sommer (eds), *EU-DSGVO und BDSG* (Frankfurt am Main: Bundes-Verlag, 2020) para. 20; Sabine Leutheusser-Schnarrenberger, 'Art. 17 GDPR', in Rolf Schwartmann/Andreas Jaspers/Gregor Thüsing/Dieter Kugelmann (eds), *DS-GVO/BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (Heidelberg: C.F Müller Verlag, 2020) para. 42; Tilman M. Dralle, 'Recht auf Löschung: der Radiergummi der DS-GVO' (2017) *BvD-NEWS* 47.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, *erasure or destruction*".[16]

Erasure is thus conceived as a data processing operation happening at the end of the data's life cycle. Art. 4 (2) GDPR distinguishes erasure and destruction as two separate operations of data processing.[17] We can observe that the few other occurrences of the term "destruction" in the legal text are systematically mentioned along with "loss" of, "alteration" of or "damage" to data and therefore related to the data's integrity.[18] The GDPR does not however elaborate on how destruction would differ from erasure. It is generally admitted that destruction refers to the idea of affecting the integrity of the data medium while erasure is a way of getting rid of data while keeping the data medium containing them usable.[19] Therefore, erasure does not need to be carried out by the annihilation of the data medium.[20]

Second, erasure has to do with the storage and the retention of data. Recital 65 GDPR provides that erasure can only be exercised if the retention of such data infringes the GDPR or a Member State's national law to which the controller is subject.[21] Erasure is therefore designed as a means to combat personal data retention when such retention is unlawful. This is in line with the principle of storage limitation enshrined in Art. 5 (e) GDPR according to which personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which said data are processed.[22] This provision implicitly states that personal data must be erased after they are no longer necessary. If the storage must be limited, erasure should have as a logical consequence that the personal data must not be stored anymore.

Such a viewpoint is also confirmed by the role that the right to erasure plays within the GDPR bundle of data subject rights. Indeed, the right to erasure can be exercised as a consequence of the successful exercise of other data subject's rights. This is

[16] Emphasis added.

[17] Jahnel, 'Art. 17 GDPR', para. 12; Däubler, 'Art. 17 GDPR', para. 20; Leutheusser-Schnarrenberger, 'Art. 17 GDPR', para. 42.

[18] Art. 4 (12); Art. 5 (1) (f); Art. 32 (2); Recital 83 GDPR.

[19] Christina-Maria Leeb/Luisa Lorenz, 'Datenschutzkonforme Dokumentenentsorgung' (2018) *Zeitschrift für Datenschutz (ZD)* 573.

[20] See definition cf. *supra* I. b.

[21] Recital 65 GDPR.

[22] Art. 5 (1) (e) GDPR.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

namely the case of the right to object which aims at the situation where the data subject at any time objects to processing of personal data at the conditions set out by Art. 21 GDPR.[23] The data subject's objection to the processing of its personal data is one of the grounds that leads to the erasure of the personal data (Art. 17 (1) (c) GDPR). Similarly, the data subject's right to withdraw its consent to the processing of its personal data (art. 7 (3) GDPR) is also one of the grounds of erasure provided in Art. 17 (1) (b) GDPR. It is worth mentioning that the right to erasure does not have the same temporal scope of application as the withdrawal of consent. Art. 17 GDPR allows the retroactive erasure of personal data which have already been collected by a controller while the revocation of one's consent to the processing of its personal data can only deploy its effect in the future (Art. 7 (3) GDPR).[24] Nevertheless, both institutions are complementary since the data subject can first withdraw its consent to the processing of its personal data for the future and then request the erasure (Art. 17 (1) (b) GDPR). Erasure is therefore a consequence of the data subject's justified objection respectively withdrawal of consent and aims at guaranteeing that personal data will not be processed further.

Third, the right to erasure (Art. 17 GDPR) must be distinguished from the right to rectification (Art. 16 GDPR). Both are indeed coexisting rights and part of the same Section 3 entitled "Rectification and erasure". The right to rectification only aims at rectifying inaccurate personal data and not having them deleted.[25] This is confirmed by a historical perspective: since the first mention of a "right to erasure" in a Council of Europe's Resolution, rectification and erasure of personal data have quite consistently been mentioned along with each other, the former applying to inaccurate or incomplete data while the second applies to obsolete and erroneous personal data.[26]

The same idea prevailed in the Data Protection Directive. Art. 6 (1) (d) of the latter stated that "Member States shall provide that personal data must be accurate and,

[23] Art. 21 (1) GDPR: "The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims".

[24] Politou/Alepis/Patsakis, 'Forgetting personal data', 7; Cesare Bartolini/Lawrence Siry, 'The right to be forgotten in the light of the consent of the data subject' (2016) *Computer Law & Security Review* 218, 228.

[25] This distinction also arises from Recital 65 GDPR.

[26] Jef Ausloos, 'The Right to Erasure in EU Data Protection Law', 93.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are *erased or rectified*".[27] Art. 5 (1) (d) GDPR provides for the same accuracy principle according to which data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay".

In short, personal data must be retained only for specific purposes and a specific period of time. Should they be inaccurate, they must be rectified and kept up to date. Should they become obsolete, they must be erased. From this perspective, erasure must be seen as a guarantee that wrong personal data will not be kept by the controller unless the latter can rectify them. There is therefore a certain proportionality to be complied with.

In a similar vein, the right to erasure must be distinguished from the right to restriction of processing in Art. 18 GDPR. The latter states that the data subject shall have the right to obtain from the controller restriction of processing on certain grounds (see Art. 18 (1) (a)-(d) GDPR). The difference with erasure is reflected in the text itself since Art. 18 (1) (b) states that a ground for restriction of processing is given when the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead. Recital 67 adds that such a right may be implemented by, *inter alia*, moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website.[28] It further clarifies that in automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed.[29]

By way of a brief interim conclusion, we can observe that erasure is not conceived on a mere structural level as it does not require that the data medium be physically annihilated but rather aims at personal data not being retained nor processed by the controller. It is therefore designed as an intermediate data processing operation which is situated between rectifying the personal data (respectively restricting its processing) and destroying the data medium. It is mainly driven by an objective of

[27] Emphasis added.

[28] Recital 67 GDPR.

[29] Recital 67 GDPR.

result which has to be interpreted in accordance with the general principles applicable to data protection. This result driven objective is in line with the technology-agnostic approach the GDPR adopts. As a consequence, the methods to reach such a result are up to the controllers which have to take into account state of the art technology.[30]

2. German Approach

While the GDPR does not define erasure, it is interesting to note that the German literature still - at least partly - relies on the definition enshrined in former versions of the German Data Protection Act[31] and extends it to Art. 17 GDPR.

The 2003 version of the German Data Protection Act ("GDPA 2003") transposing the right to erasure provided in Art. 12 (c) DPD was conceived as a personal data processing operation. Indeed, § 3 (4) [5] GDPA 2003 states that "Processing is the storage, modification, transmission, blocking and erasure of personal data. [...] In particular, regardless of the applicable procedure, erasure is the *rendering of stored personal data unrecognizable*[32]".[33] This version used the word "*Unkenntlichmachen*", which is a compound word that literally means "to make [the data] unrecognizable".

Interestingly, this specific wording can be traced back to the original version of the German Data Protection Act ("GDPA 1977").[34] It remained unchanged since, despite the advent of widespread internet access and multinational corporations routinely handling massive amounts of personal data.

In 2018, Germany enacted a new version of its German Data Protection Act[35] ("GDPA 2018") in order to align with and apply the GDPR[36] and now provides for a

[30] Recital 66 GDPR.

[31] *Bundesdatenschutzgesetz* in the original German.

[32] Emphasis added.

[33] Free translation of «Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten ».

Arning, 'Art. 17 GDPR', para. 410; Sascha Kremer, 'Art. 17 GDPR', in Philipp Laue/Sascha Kremer (eds), *Das neue Datenschutzrecht in der betrieblichen Praxis* (Baden-Baden: Nomos, 2019), para. 47; Leutheusser-Schnarrenberger, 'Art. 17 GDPR', para. 42.

[34] § 2 (2) [4] GDPA 1977: « *Im Sinne dieses Gesetzes ist* [...] *Löschen (Löschung) das Unkenntlichmachen gespeicherter Daten* [...] ».

[35] German Data Protection Act of 30 June 2017.

[36] German Parliament (*Bundestag*), 'Draft Act of 24 February 2017 on the Adaptation of Data Protection Law to Regulation (EU) 2016/679 and the Implementation of Directive (EU) 2016/680,

right to erasure ("*Recht auf Löschung*") independent from the right to access in its § 35 GDPA 2018. However, the definition of erasure enshrined until then has been removed and the current version leaves open what erasure means.

Notwithstanding its removal, scholars and data protection authorities still widely rely on the original definition when it comes to erasure within the meaning of the GDPR.[37] In a guideline of the data protection commissioner of the State of Mecklenburg-Vorpommern, erasure in the sense of Art. 17 GDPR is defined as the act of rendering data unrecognizable ("*Der Begriff „Löschen" beschreibt das Unkenntlichmachen gespeicherter personenbezogener Daten*").[38] More recently, in a Guidance on the right to erasure under the GDPR issued on 1 June 2022, the Data Protection Commissioner of the State of Bavaria adopted a slightly different wording stating that data must be made unusable ("*unbrauchbar*") in such a way that the creation of new personal reference is excluded.[39]

We can also observe that in the German approach, no methods are imposed on the controllers and erasure is defined in terms of results.

C. Implementing Erasure

Although we have determined that erasure should be considered in terms of its results, the interpretation of what should be understood as being the result is subject to debate and different points of view. With that in mind, we can observe mainly two

Document 18/11325' (*Deutscher Bundestag, Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, Drucksache 18/11325, 24. Februar 2017*), 105.

[37] Armin Fladung, 'Art. 17 GDPR', in Tim Wybitul (ed.), *Handbuch EU-Datenschutz-Grundverordnung* (Frankfurt am Main: Recht und Wirtschaft, 2017), para. 4; Arning, 'Art. 17 GDPR', para. 410. See also Däubler, 'Art. 17 GDPR', para. 20; Marian Alexander Arning, in Flemming Moos/Jens Schefzig/Marian Alexander Arning (eds), *Die neue Datenschutz-Grundverordnung* (Berlin: De Gruyter, 2018), § 6 para. 11; Leutheusser-Schnarrenberger, 'Art. 17 GDPR', para. 42; Data Protection Commissioner of the German State of Mecklenburg-Vorpommern, 'Module 60 "Erasure and Destruction" of 2 September 2020' (*Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Standard-Datenschutzmodell, Baustein 60 "Löschen und Vernichten" (Version 1.0a vom 2 September 2020*), 1; Tilman M. Dralle, 'Recht auf Löschung: der Radiergummi der DS-GVO', 47.

[38] Data Protection Commissioner of the German State of Mecklenburg-Vorpommern, 'Module 60 "Erasure and Destruction" of 2 September 2020', 1.

[39] Data Protection Commissioner of the German State of Bavaria, 'Guidelines to the Right to Erasure of 1 June 2022' (Der Bayerische Landesbeauftragte für den Datenschutz, Das Recht auf Löschung nach der Datenschutz-Grundverordnung, Orientierungshilfe, 1. Juni 2022), 31 para. 54.

distinct schools of thoughts: one in favor of an irreversible erasure (cf. *infra* 1.), the other in favor of a proportionate erasure (cf. *infra* 2.).[40]

Both approaches aim at a different level of result and, as a consequence, promote different ways of erasing the personal data. While we present the main characteristics and the inherent pitfalls of these two perspectives in separate subsections, it shall be noted that the borders between both approaches are not necessarily as strict and clear; some actors may rely on erasure methods arising from both schools of thoughts, be it because of a lack of understanding of the technical differences, misuse of language or for mere practical reasons.[41] Furthermore, it is worth pointing out that German opinions are overrepresented because of their important doctrinal production on the GDPR.

1. Irreversible Approach

One approach to data erasure is to consider that the result should be irreversible. According to this school of thought, erasure needs to be implemented in the way of an irreversible process which consists in rendering personal data no longer usable, readable and processable.[42] The advocates of this approach recommend a *physical erasure* of the personal data.

Physical erasure can be carried out in different ways. It can be performed by *the destruction of the data medium* itself.[43] Regarding data in the analog form, the ways to erase them are quite well established. When it comes to data on paper, it is generally suggested that redacting, burning or shredding personal data is an efficient

[40] Sven Hunzinger, 'Das Löschen im Datenschutzrecht' (Frankfurt: Nomos, 2018), 59 ff.

[41] The references also suggest that the irreversible approach was initially considered prior to the GDPR.

[42] Leutheusser-Schnarrenberger, 'Art. 17 GDPR', para. 42; Dix, 'Art. 17 GDPR', para. 5; Däubler, 'Art. 17 GDPR', para. 20; Tilman M. Dralle, 'Recht auf Löschung: der Radiergummi der DS-GVO', 47; Wulf Kamlah, 'Art. 17 GDPR', Kai-Uwe Plath (ed.), *DSGVO/BDSG/TTDSG, Kommentar* (Köln: Dr. Otto Schmidt, 2023), para. 2. See also Sven Hunzinger, 'Das Löschen im Datenschutzrecht', 59 ff; State Social Court of Bayern (*Bayerisches Landessozialgericht*), decision L 15 SB 80/06 of 31 March 2011 (2011) *Beck-Rechtsprechung* 75017; Administrative Court of Karlsruhe (*Verwaltungsgericht Karlsruhe*), decision 2 K 3249/12 of 27 May 2013 (2013) *Neue Zeitschrift für Verwaltungsrecht Rechtsprechungs-Report* 797; Austrian Supreme Court (*Österreichischer Oberster Gerichtshof*), decision 6 Ob 41/10p of 15 April 2010 (2011) *Multimedia und Recht* 204.

[43] Arning, 'Art. 17 GDPR', para. 410; Leutheusser-Schnarrenberger, 'Art. 17 GDPR', para. 43; Dix, 'Art. 17 GDPR', para. 5; Däubler, 'Art. 17 GDPR', para. 20. See also the Danish Data Protection Authority of September 2014, 'Guidelines to Personal Data Erasure' (*Datatilsynet, It-sikkerhedstekst ST3, Sletning af personoplysninger*, September 2014), 2.

way to erase them. The German legal literature[44] generally refers to the DIN-66399 standard[45] designed by the *Deutsches Institut für Normung* (DIN) which is the German national organization for standardization and the German ISO member body.[46] This standard is designed for the destruction of the data medium (*DIN-Norm zur Datenträgervernichtung*).[47] Although it was developed for the 2009 version of the GDPA, scholars also refer to it for erasure under the GDPR.[48] When it comes to digital data, several data protection authorities suggest that the destruction of a digital data medium through mechanical shredding, melting or burning, may be a solution when erasure cannot be ensured effectively.[49]

Another way to physically erase data is the *overwriting of the data.*[50] Overwriting consists in using the same space on the data medium to store other data. It is generally accepted that multiple overwrites making the data unrecognizable erasure satisfies the expected standards.[51] The Irish Data Protection Commission recommends for instance that hard drives be overwritten between three and five times, depending on the sensitivity of the personal data stored.[52]

Furthermore, several Data Protection Commissioners suggest that, instead of destroying the data medium or overwriting the personal data, a *degaussing* of the data

---

[44] Matthias Enzmann/Annika Selzer/Dominik Spychalski, 'Data Erasure under the GDPR – Steps towards Compliance' (2019) *European Data Protection Law Review* 416, 419; Leeb/Lorenz, 'Datenschutzkonforme Dokumentenentsorgung', 577.

[45] Deutsches Institut für Normung, 'DIN 66399' <https://din66399.eu> accessed 23 May 2025.

[46] Deutsches Institut für Normung, 'Setting standards with DIN' <https://www.din.de/en/din-and-our-partners/din-e-v/din-what-we-do> accessed 23 May 2025.

[47] Deutsches Institut für Normung, 'DIN 66399' <https://din66399.eu> accessed 23 May 2025.

[48] Eva Gardyan-Eisenlohr/Cay Lennart Cornelius, 'Datenlöschung' in Flemming Moos/Jens Schefzig/Marian Alexander Arning (eds), *Praxishandbuch DSGVO* (Frankfurt am Main: Recht und Wirtschaft, 2021), § 12 para. 38; Leeb/Lorenz, 'Datenschutzkonforme Dokumentenentsorgung', 577.

[49] Data Protection Commissioner of the German State of Mecklenburg-Vorpommern, 'Module 60 "Erasure and Destruction" of 2 September 2020', 3; Danish Data Protection Authority of September 2014, 'Guidelines to Personal Data Erasure' (*Datatilsynet, It-sikkerhedstekst ST3, Sletning af personoplysninger*, September 2014), 2.

[50] Arning, 'Art. 17 GDPR', para. 410; Leutheusser-Schnarrenberger, 'Art. 17 GDPR', para. 43; Dix, 'Art. 17 GDPR', para. 5.

[51] Däubler, 'Art. 17 GDPR', para. 20; Arning, 'Die neue Datenschutz-Grundverordnung', § 6 para. 211. See also Data Protection Commissioner of the German State of Mecklenburg-Vorpommern, Module 60 "Erasure and Destruction" of 2 September 2020, 3.

[52] Irish Data Protection Commission, 'Guidance Note: Guidance for Controllers on Data Security of February 2020', 11.

medium can also be performed.[53] On specific data media that store data magnetically, degaussing means erasing the data by altering the magnetic properties of the medium.

Some pitfalls must be considered in relation to the irreversible approach. Although irreversible erasure seems like a really clean and clear-cut way of ensuring erasure, the fact that a method constitutes physical erasure does not necessarily provide absolute guarantees.[54] For example, overwriting data may be imperfect and still reversed with some advanced data recovery techniques, whereas melting a hard drive has far less chances of being undone.

In turn, physical erasure, especially in its most radical forms, is impractical to implement in this way. If an entire storage medium has to be destroyed in order to erase some particular data, then that affects all of the other data on that medium too. This means that the cost and consequences may sometimes be prohibitive too and therefore the imperative to erase some data has to be weighed against other considerations. For example, if one is to shred a storage device from a hospital's infrastructure because it contains some particular person's patient data that needs to be erased, then that procedure will also destroy the data of some other patients that just happen to be stored on that same data medium.

2. Proportionate Approach

A competing view on the implementation of erasure is that it is sufficient if the result of the erasure process is that the data cannot be retrieved except with

[53] Data Protection Commissioner of the German State of Sachsen, '10th Activity Report of 1 September 2011' (Landesbeauftragter für den Datenschutz Sachsen, X. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz, 1. September 2011), 100, para. 14.2; Irish Data Protection Commission, 'Guidance Note: Guidance for Controllers on Data Security of February 2020', 11.

[54] Regarding the subtleties of overwriting, the reader can refer to Nikolai Joukov/Harry Papaxenopoulos/Erez Zado, 'Secure Deletion Myths, Issues, and Solutions' (2006) *Proceedings of the second Association for Computing Machinery workshop on Storage security and survivability* 61, 62.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

disproportionate effort.[55] According to this point of view, there is still a theoretical possibility of retrieving the data.[56]

Such a proportionate erasure can be carried out through logical erasure, anonymization or encryption.

Logical erasure[57] consists in rendering data irretrievable by purely software means.[58] This does not lead to the actual deletion of the personal data but instead makes the personal information more difficult to be recovered and retrieving it requires significant expert knowledge.[59] In that respect, the German legal literature refers to the DIN-66398 standard which is since 2016 a guideline that designs requirements for an efficient erasure concept complying with data protection laws.[60] One can also now rely on the ISO/IEC 27555:2021 norm which is a guideline on "personally identifiable information deletion" that derives directly from the DIN standard.[61] The ISO standard defines "deletion" as "process by which personally identifiable information (PII) is changed so that it is no longer present or recognizable and usable and can only be reconstructed with excessive effort".[62]

---

[55] Arning, 'Art. 17 GDPR', para. 410; Tobias Herbst, 'Art. 17 GDPR', in Jürgen Kühling/Benedikt Buchner (eds), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Kommentar* (Munich: C.H Beck, 2020), paras. 37 ff; Alexander Roßnagel, 'Datenlöschung und Anonymisierung' (2021) *Zeitschrift für Datenschutz*, 189; Jan Geert Meents/Britta Hinzpeter, 'Art. 17 GDPR', in Jürgen Taeger/Detlev Gabel (eds), *DSGVO – BDSG – TTDSG, Kommentar* (Frankfurt am Main: Recht und Wirtschaft, 2022), para. 74; Christoph Worms, 'Art. 17 GDPR', in Heinrich Amadeus Wolff/Stefan Brink (eds), *Datenschutzrecht, Kommentar* (Munich: C.H Beck, 2022), para. 55; Boris P. Paal, 'Art. 17 GDPR', in Boris P. Paal/Danuel A. Pauly (eds), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Beck'sche Kompakt-Kommentare* (Munich: C.H Beck, 2018), para. 30; Enzmann/Selzer/Spychalski, 'Data Erasure under the GDPR', 419.

[56] Paal, 'Art. 17 GDPR', para. 30.

[57] See Athanassoulis/Sarkar/Papon/Zhu/Staratzis, 'Building Deletion-Compliant Data Systems', 22 ff.

[58] Enzmann/Selzer/Spychalski, 'Data Erasure under the GDPR', 419; Jahnel, 'Art. 17 GDPR', para. 13; Arning, 'Art. 17 GDPR', para. 410; Arning, 'Die neue Datenschutz-Grundverordnung', § 6 para. 11. See also David Rosenthal, 'Löschen und doch nicht löschen' (2019) *Digma* 190, 194.

[59] Dix, 'Art. 17 GDPR', para. 5.

[60] Eva Gardyan-Eisenlohr/Cay Lennart Cornelius, 'Datenlöschung', § 12 para. 38.

[61] International Organization for Standardization, 'ISO/IEC 27555:2021(en) - Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion' <https://www.iso.org/obp/ui/#iso:std:iso-iec:27555:ed-1:v1:en> accessed 23 May 2025.

[62] *Ibid.* For a more in-depth analysis of the slight differences between both standards, see Deutsches Institut für Normung, 'ISO/IEC 27555 und die Bezüge zur DIN 66398' <https://www.din-66398.de/inhalt/bezuege/std/b_s_iso27555.html> accessed 23 May 2025.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

Proportionate erasure of data can also be carried out by *anonymization*[63] or *encryption*[64]. Personal data that are, by hypothesis, definitively anonymized, fall outside the scope of the regulation.[65] The required level of anonymization, whether it should consist in absolute anonymity or mere factual anonymity[66], is not quite consensual in the legal literature.[67]

It is worth mentioning that some isolated viewpoints are even more liberal and suggest that it is sufficient to render the data "unusable for ordinary use" (e.g. retrieval via a customer database) or that erasure of all available backup copies are not required.[68]

As is the case with the irreversible approach, there are some pitfalls to consider.[69] First of all, it is much harder to prove digital erasure than is the case with erasure of analog data[70]. A trusted third party can observe paper documents being burnt, for example. For logical erasure of digital data, it is very impractical to guarantee that a manipulation done with software indeed performs what is intended. In practice, some degree of trust in the data controller is necessary. While not a problem in itself, this is an often-overlooked property of software, and it should be taken into account when designing legislation and especially when designing data erasure procedures and best

[63] In an administrative decision rendered in Austria, the Austrian Data Protection Authority held that the removal of the personal reference through the process of anonymization was a possible means of erasure within the meaning of Art. 17 GDPR, provided that neither the controller itself nor a third party can retrieve personal data without disproportionate effort. See Austrian Data Protection Authority (*Österreichische Datenschutzbehörde*), decision DSB-D123.270/0009-DSB/2018 of 5 December 2018.

[64] Arning, 'Art. 17 GDPR', para. 410; Jahnel, 'Art. 17 GDPR', para. 13; Däubler, 'Art. 17 GDPR', paras. 20, 23; Meents/Hinzpeter, 'Art. 17 GDPR', para. 75

[65] Recital 26 GDPR.

[66] Factual anonymity means anonymity achieved by methods that are deemed to not be reversible using reasonable resources or in a relevant time frame. Note that from a technical perspective absolute anonymity, as opposed to factual anonymity, may only be achieved under strong mathematical assumptions but discussing this distinction is outside the scope of this contribution.

[67] Arning, 'Art. 17 GDPR', para. 410 and the references in note 697. See among other opinions: Roßnagel, 'Datenlöschung und Anonymisierung', 189; Jahnel, 'Art. 17 GDPR', para. 13; Verena Stürmer, 'Löschen durch Anonymisieren? Mögliche Erfüllung der Löschpflicht nach Art. 17 DS-GVO' (2020) *Zeitschrift für Datenschutz,* 626; Hunzinger, 'Das Löschen im Datenschutzrecht', 101.

[68] See for instance Niko Härting, 'Datenschutz-Grundverordnung' (Köln: Dr. Otto Schmidt, 2016), para. 701.

[69] See also Athanassoulis/Sarkar/Papon/Zhu/Staratzis, 'Building Deletion-Compliant Data Systems', 25.

[70] Politou/Alepis/Patsakis, 'Forgetting personal data', 13.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

practices. Even if the burden of proof is placed on the data controller, the problem remains. It is hard to prove that some piece of data has been erased.[71]

Moreover, as digital copies are trivial to make, indistinguishable from the original and easy to transport, across the internet for example, it can be easy to circumvent erasure mandates by simply stashing away copies of the data. In some cases, these copies can even be kept in different jurisdictions, very easily.

Finally, it is hard to make lasting hypotheses about reversibility since some of the techniques discussed, such as anonymization and encryption are the subject of active research and technological developments and will continue to be so for the foreseeable future. New discoveries and developments may invalidate some of the assumptions made at the time of erasure.[72] For example, some state-of-the-art encryption techniques that have been considered practically unbreakable for decades will be trivial to crack with the advent of quantum computing.[73] There is therefore an inherent risk in pursuing erasure through anonymization or encryption and it is therefore key to ensure that the cost-benefit analysis[74] takes all these factors into account, through deep understanding of the mathematical and technical considerations.

---

[71] Oliver Stutz, '8. Datenlöschung', in Uwe Schläger/Jan-Christoph Thode (eds), *Handbuch Datenschutz und IT-Sicherheit* (Berlin: Erich Schmidt Verlag, 2022), paras. 196 f.

[72] Examples of re-identification of anonymized datasets range from a streaming platform's user data (e.g. Arvind Narayanan/Vitaly Shmatikov, 'Robust De-anonymization of Large Sparse Datasets' (2008) *Institute of Electrical and Electronics Engineers (IEEE) Symposium on Security and Privacy* 111) to the re-identification of genomic data (e.g. Malin Bradley/Latanya Sweeney, 'How (not) to protect genomic data privacy in a distributed network: using trail reidentification to evaluate and design anonymity protection systems' (2004) *Journal of Biomedical Informatics* 179) all the way to de-anonymization techniques based on cross-referencing medical and voter databases (e.g. Latanya Sweeney, 'Weaving Technology and Policy Together to Maintain Confidentiality' (1997) *Journal of Law, Medicine & Ethics* 98).

[73] The security of some of the most widely used cryptosystems, such as RSA, relies on the fact that tremendous computational power is required to find the prime factorization of some judiciously chosen numbers (see Patent US-4405829-A). It turns out that, there is a known method called Schor's algorithm (e.g. Peter W. Shor, 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer' (1997) *SIAM Journal on Scientific and Statistical Computing* 1484), which provided a quantum computer efficiently solves this factorization task and thus compromises the security of RSA and other schemes relying on the same mathematical principles.

[74] On the different views regarding the risk level required for erasure and anonymization from a legal perspective: Stürmer, 'Löschen durch Anonymisieren?', 629; Roßnagel, 'Datenlöschung und Anonymisierung', 191.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

III. Swiss Data Protection Act

A. Current Legislative Context in Switzerland

The first version of the SDPA was published on 1 July 1993.

Although the SDPA was enacted because of the emergence of information technologies, it still enshrines a principle of technological neutrality.[75] It is indeed not based on specific technical concepts and remains neutral in the context of technological developments.[76] Therefore, similarly to the GDPR, the SDPA does not distinguish between manual and automated data processing and does also encompass mixed forms of data processing.[77]

A revised version of the SDPA came into force on 1 September 2023 after a long and extensive revision. The latter aims to adapt the Swiss data protection law to the evolving technological circumstances, strengthen the position of the data subject as well as align with respectively bring closer to the current European legal texts (Art. 4 (2)) as well as the Convention 108 (Art. 2 (b)).[78] It is in line with the need for the Swiss economy to benefit from a legal framework that guarantees a sufficient level of data protection in order to benefit from an EU adequacy decision as well as allow cross-border data communication without additional requirements (see Art. 45 GDPR).

---

[75] Swiss Federal Council, 'Message of 23 March 1988 on the Swiss Data Protection Act', Federal Gazette 1988 II 413 (*Schweizer Bundesrat, Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, Bundesblatt (BBl) 1988 II 413*), 425: "the installation of automated data processing allows for the exploitation of the information with a systematic and an efficiency unknown until then. It is nowadays [i.e. in 1988] possible to collect, gather, process and disseminate information almost without limits. Modern technology makes it possible to connect files to each other, to split them up, to process them and to transmit their content at will. These processing possibilities are expected to increase further with the rise of telematics, i.e the combination of automated data processing and telecommunication technology. There is no longer any obstacle to the creation of local, regional and international networks connecting geographically distant computing centers and data sets" (free translation from the French version).

[76] Swiss Federal Council, 'Message of 1988', 424 ff.

[77] Swiss Federal Council, 'Message of 1988', 424 ff.

[78] Sandra Husi-Stämpfli, 'Entstehungsgeschichte', in Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (eds), *Datenschutzgesetz* (Bern: Staempfli, 2023), para. 11; Rudin, 'Art. 5 SDPA' in Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (eds), *Datenschutzgesetz* (Bern: Staempfli, 2023), para. 43. Swiss Federal Office of Justice, 'Stärkung des Datenschutzes - Totalrevision des Bundesgesetzes über den Datenschutz (DSG)', <https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/archiv/datenschutzstaerkung.html> accessed 23 May 2025.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

In the context of this amendment, it is particularly relevant to present the characteristics of the right to erasure in the light of the former (cf. *infra* B) and revised (cf. *infra* C) versions of the SDPA.

B. Under the Former SDPA

1. Right to Destruction

Until 31 August 2023, Art. 15 (1) of the former Swiss Data Protection Act ("fSDPA") provided, in the context of personal data processed by private persons, that a data subject may request that personal data be corrected or destroyed (Art. 15 (1) fSDPA). Similarly, when the personal data was processed by a federal body, the data subject could request the latter to correct or destroy the personal data (Art. 25 (3) (a)) fSDPA.

As reflected in the aforementioned provisions, neither contained a right to erasure. The fSDPA relied – at least from a linguistic perspective – exclusively on the notion of destruction.[79] It allowed for a right to rectification and a right to destruction of data. The interplay between the right to rectification and the right to destruction was based on a gradation and the respect of the principle of proportionality: where data were inaccurate, the data subject could request that they be corrected; where the processing was unlawful, the data subject could request the destruction. Destruction therefore was an *ultima ratio.*[80] If some forms of processing were lawful, the controller could only be ordered to stop the unlawful processing, and further processing was allowed for the remainder.[81] The right to destruction of personal data was thus subsidiary to the correction of said data: it only applied when the personal data was totally erroneous, and that rectification was not sufficient to remedy the violation.[82]

It is interesting to mention that during the legislative process leading to the enactment of the first version of the SDPA, it was discussed whether the term "destruction"

[79] There was however a single occurrence of "erasure" which was reflected in the French ("*effacé*") and Italian ("*cancellati*") versions of Art. 5 fSDPA (Art. 5 (3) fSDPA: "[c]*elui qui traite des données personnelles doit s'assurer qu'elles sont correctes. Il prend toute mesure appropriée permettant* d'effacer *ou de rectifier les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées*" (Emphasis added). The German and English versions (however the latter has no legal force as English is not an official language of Switzerland) of the text used the words "*vernichtet werden*" respectively "destroyed". This inconsistency is most likely due to poor translation (see Rosenthal, 'Löschen und doch nicht löschen', para. 11).

[80] Eva Cellina, 'La commercialisation des données personnelles' (Geneva: Schulthess, 2020), para. 1462; Philippe Meier, 'Protection des données' (Bern: Staempfli, 2010), para. 1746.

[81] Meier, 'Protection des données', para. 1746.

[82] Cellina, 'La commercialisation des données personnelles', para. 1462.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

should be removed from the definition of data processing given the practical hurdles that may stand in the way of such a strict approach.[83] It was eventually decided to maintain the notion in the definition with the idea that it would strengthen the confidentiality of sensitive data.[84] The idea was thus to prevent situations in which sensitive paper documents would be disposed of in a waste basket without first being made unreadable by a shredder or in which digital data would be only apparently erased because the computer does not overwrite the data but only marks them as deleted.[85]

In practice however, the notion of erasure (*effacement des données*; *Löschung von Daten*) was regularly interchanged with that of destruction[86] and both were often used as synonyms.[87]

2. Defining and Implementing Destruction

Destruction was defined in the legal literature as the act of irreversibly removing personal data from a data file.[88] Similarly to what prevails for erasure in the GDPR,

---

[83] Gabor-Paul Blechta, 'Art. 3 fSDPA', in Urs Maurer-Lambrou/Gabor-Paul Blechta (eds), *Datenschutzgesetz/Öffentlichkeitsgesetz* (Basel: Helbing Lichtenhahn, 2014), para. 75; David Rosenthal, 'Art. 3 fSDPA' in David Rosenthal/Yvonne Jöhri (eds), *Handkommentar zum Datenschutzgesetz* (Geneva/Basel/Zurich: Schulthess, 2008), para. 65.

Art. (3) (f) fSDPA, contrary to the corresponding definition in the GDPR, did only contain the notion of destruction: "any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or *destruction* of data" (Emphasis added).

[84] Blechta, 'Art. 3 fSDPA', para. 75.

[85] Blechta, 'Art. 3 fSDPA', para. 75; Rosenthal, 'Art. 3 fSDPA', para. 65. See also Martin Winterberger-Yang, 'Art. 21 fSDPA', in Urs Maurer-Lambrou/Nedim Peter Vogt (eds), *Datenschutzgesetz* (Basel: Helbing Lichtenhahn, 2006), para. 10.

[86] See for example François Bohnet, 'Actions civiles', volume 1 (Basel: Helbing Lichtenhahn, 2019), § 4 para. 52. In the same vein, see Meier, 'Protection des données', paras. 1746, 1748.

[87] Marnie Kiener, 'Datenlöschung einer Bank im Lichte der Datenschutzgesetzgebung Schweiz und EU' (Zurich: Schulthess, 2023), 37.

[88] Robert Bühler, 'Art. 21 fSDPA' in Urs Maurer-Lambrou/Gabor-Paul Blechta (eds), *Datenschutzgesetz/Öffentlichkeitsgesetz* (Basel: Helbing Lichtenhahn, 2014), para. 14; Yvonne Jöhri, 'Art. 21 fSDPA' in David Rosenthal/Yvonne Jöhri (eds), *Handkommentar zum Datenschutzgesetz* (Geneva/Basel/Zurich: Schulthess, 2008), para. 25; Fey, 'Art. 21', in Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (eds), *Datenschutzgesetz* (Bern: Staempfli, 2015), para. 13; Beat Rudin, 'Art. 3 fSDPA', in Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (eds), *Datenschutzgesetz* (Bern: Staempfli, 2015), para. 39; Hans Bättig, 'Art. 21 fSDPA', in Urs Maurer-Lambrou/Nedim Peter Vogt (eds), *Kommentar zum schweizerischen Datenschutzgesetz* (Basel: Helbing Lichtenhahn, 1995), para. 15; Winterberger-Yang, 'Art. 21 fSDPA', para. 10. In the same vein: Rosenthal, 'Art. 3 fSDPA', para. 65.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

this definition relied on the result and the methods were up to the controllers.[89]

Regarding the implementation, it was suggested to distinguish between paper and digital data.[90] When it came to analog data in the form of paper, they had to be destroyed by shredding or burning so that third parties had no more access to the information.[91] There was awareness that such an approach to erasure is not trivial and may require considerable efforts that every processor is not necessarily prepared to undertake.[92] For digital data, authors advocated for a physical erasure of the data and, when necessary, the destruction of the data medium.[93] Ordinary deletion commands or mere reformatting of data medium did not constitute destruction in the sense of the fSDPA.[94] Back-up copies of the data also had to be destroyed, regardless of how many of those existed.[95] In order to take into account technological evolution, if technical progress made it possible to retrieve personal data that has been destroyed, the data had to be destroyed again.[96]

In Switzerland, a landmark decision on the federal level dealing with the implementation of data erasure as conceived under the fSDPA concerned a case of international administrative assistance in tax matters in which the plaintiffs requested the immediate destruction of personal data and bank documents collected by the Federal Tax Administration because such data were collected unlawfully. Founding in favor of the plaintiffs, the Swiss Federal Administrative Court ("SFAC") held that it was appropriate to destroy the personal data at issue. As a principle for the destruction of data, it stated that the destruction of personal data meant that these

[89] Bühler, 'Art. 21', para. 14; Rudin, 'Art. 3 fSDPA', para. 39.

[90] Bühler, 'Art. 21 fSDPA', para. 14; Fey, 'Art. 3 fSDPA', para. 39; Winterberger-Yang, 'Art. 21 fSDPA', para. 10

[91] Bühler, 'Art. 21 fSDPA', para. 15; Bättig, 'Art. 21 fSDPA', paras. 15, 17.

[92] Bühler, 'Art. 21 fSDPA', para. 14.

[93] Bühler, 'Art. 21 fSDPA', para. 14; Jöhri, 'Art. 21 fSDPA', para. 25; Winterberger-Yang, 'Art. 21 fSDPA', para. 10.

[94] Bühler, 'Art. 21 fSDPA', para. 14; Jöhri, 'Art. 21 fSDPA', para. 25.

[95] Bühler, 'Art. 21 fSDPA', para. 14; Jöhri, 'Art. 21 fSDPA', para. 25; Bättig, 'Art. 21 fSDPA', para. 16.

[96] Jöhri, 'Art. 21 fSDPA', para. 25.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

had to be permanently destroyed and irreversibly eliminated[97]. Since only data in the digital form was involved, the SFAC held that the situation was more complex than when it comes to paper data. It stated that it was essential to know how the data were recorded by the controller and how it was obtained.[98] If the data was transmitted to the controller by means of a CD or a USB stick[99], the data medium must, on the one hand, be rendered unusable by means of a perforation and, on the other hand, all copies (including all back-ups) must be handled in such a way that the data were no longer readable.[100] If data was sent to the controller as an attachment to an email, any intermediate records of this email must also have been destroyed.[101] The SFAC specified that as recording techniques change regularly, high standards must be set for destruction.[102] It further clarified that ordinary deletion, mere reformatting and deletion of passwords did constitute not destruction in the sense of the fSDPA.[103]

In the light of the notion of destruction enshrined in the fSDPA, the SFAC clearly opted for the irreversible approach, thus aligning with the prevailing legal doctrine. Some authors were aware that such an implementation required important technical (e.g. having the appropriate equipment) and/or organizational (supervised disposal of paper documents) measures when it came to paper data.[104] This irreversible approach still permeates the recent data protection legal literature.

---

[97] Swiss Federal Administrative Court (*Bundesverwaltungsgericht*), decision BVGE 2015/13 of 23 April 2015 (published in German). A French translation is available in (2016/I) *Journal des Tribunaux* 229 ff.

[98] Swiss Federal Administrative Court (*Bundesverwaltungsgericht*), decision BVGE 2015/13 of 23 April 2015, para. 3.3.4.

[99] It is apparent that even when applying a technologically neutral drafted law, the courts have to be more specific when it comes to the implementation and setting guidelines. The risk is that such instructions may rapidly become obsolete, in this instance if CDs and USB sticks fall out of use in favor of other data mediums. Moreover, in this particular case, thanks to built-in error correction codes (see ISO/IEC 10149:1995, 30 f, Annex C), it turns out that perforating a CD may not impact the data on it in a lot of cases.

[100] Swiss Federal Administrative Court (*Bundesverwaltungsgericht*), decision BVGE 2015/13 of 23 April 2015, para. 3.3.4.

[101] Swiss Federal Administrative Court (*Bundesverwaltungsgericht*), decision BVGE 2015/13 of 23 April 2015, para. 3.3.4.

[102] Swiss Federal Administrative Court (*Bundesverwaltungsgericht*), decision BVGE 2015/13 of 23 April 2015, para. 3.3.4.

[103] Swiss Federal Administrative Court (*Bundesverwaltungsgericht*), decision BVGE 2015/13 of 23 April 2015, para. 3.3.4.

[104] Blechta, '3 fSDPA', para. 75.

Regarding digital data, we refer to our considerations on the pitfalls regarding the irreversible approach under EU law (cf. *supra* II C. 1). Those also apply to the Swiss approach to destruction under the fSDPA.

C. Under the Current SDPA

1. Right to Erasure

One of the main novelties of the SDPA is the introduction of an explicit right to erasure, a legal entity which has to be distinguished from the right to destruction which prevailed under the fSDPA.[105] In the context of the processing of personal data by private persons, Art. 32 provides that the data subject may lodge actions towards the protection of its personality in case of unlawful processing.[106] The data subject may, in particular, request the erasure or destruction of its personal data (Art. 32 (2) (c) SDPA). A similar rule is provided for in the context of the processing of personal data by federal bodies in Art. 41 SDPA.[107]

As a result of this addition, the notion of erasure now appears in several instances in the SDPA. Erasure has also been included in the definition of "data processing" in addition to the "destruction" of personal data (compare with footnote 83), similarly to what is provided for in Art. 4 (2) GDPR.[108] Moreover, erasure and destruction are regularly mentioned next to each other as alternative data processing operations (see Art. 5 (d), 5 (h), 6 (5), 32 (2) (c), 32 (4), 41 (2), (3) and (5) SDPA). Notwithstanding this, the text neither defines what erasure nor destruction of personal data means.[109]

[105] The available English translation of the SDPA uses the term "deletion" but for the sake of consistency, we use hereafter that of erasure.

[106] Sylvain Métille, 'La (nouvelle) loi fédérale sur la protection des données du 25 septembre 2020', in Astrid Epiney/Sophie Moser/Sophia Rovelli (eds), *La Révision de la Loi fédérale sur la protection des données* (Zurich: Schulthess, 2022), 21.

[107] When personal data processing is carried out by federal bodies, the SDPA allows the latter - under certain conditions - to opt for the limitation of processing which is a milder measure than erasure or destruction and allows said bodies to continue processing data for the specific purposes that hindered their erasure, cf. Métille, 'La (nouvelle) loi fédérale sur la protection des données', 21 f.

[108] Art. 5 (d) SDPA: "processing means any handling of personal data, irrespective of the means and procedures used, in particular the collection, storage, keeping, use, modification, disclosure, archiving, deletion or destruction of data".

[109] Rudin, 'Art. 5 SDPA', para. 43.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

2. Defining and Implementing Erasure

One can wonder to what extent the now express mention of two coexisting notions aims at materializing their substantive differences and to what extent they will align with the corresponding notions in the GDPR.

Taking a look at the preparatory work, we see that the message from the Federal Council to the national Parliament regarding the SDPA introduces a distinction between both notions when it comes to the result of their implementation. On the one hand, the meaning of destruction remains the same as under the former version and means that the personal data must be rendered irreversibly unreadable.[110] On the other hand, it states that erasure refers to "usual deletion orders or pure reformatting".[111] The so far emerging doctrine regarding the revised version of the SDPA seems to embrace this view.[112] Some authors suggest that erasure is successfully implemented when no further reference to a person can be made.[113]

We can observe that Switzerland adopts - maybe somewhat unwittingly - a differentiated approach in the wake of the revised version of the SDPA. The so far prevailing approach to the implementation of erasure does not align with the latest developments in European law. According to our understanding of the Swiss point of view, the notion of destruction encompasses the hypotheses of physical erasure

---

[110] Swiss Federal Council, 'Message of 15 September 2017 on the Federal Act on the total revision of the Federal Data Protection Act and on the amendment of other federal acts' Federal Gazette 2017 6565 (*Schweizer Bundesrat, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, Bundesblatt (BBl) 2017 6565*), 6641.

[111] Swiss Federal Council, 'Message 2017', 6641. Free translation of the original passage in French: "[l]es ordres habituels de suppression ou un pur reformatage ne représentent pas une destruction, mais un effacement".

[112] Rudin, 'Art. 5 SDPA', paras. 43 ff; Benjamin Domenig/Christian Mitscherlich/Chantal Lutz, 'Datenschutzrecht für Schweizer Unternehmen, Stiftungen und Vereine' (Bern: Staempfli, 2022), para. 485; Philippe Meier/Nicolas Tschumy 'Art. 5 SDPA', in Philippe Meier/Sylvain Métille (eds), *Loi fédérale sur la protection des données* (Basel: Helbing Lichtenhahn, 2023), para. 75; Emilie Jacot-Guillarmod, 'Art. 5 SDPA', in Yaniv Benhamou/Bertil Cottier (eds), *Loi fédérale sur la protection des données* (Basel: Helbing Lichtenhahn, 2023), para. 39. In the same vein: David Rosenthal/Samira Studer/Alexandre Lombard, 'La nouvelle loi sur la protection des données', *Jusletter of 12 April 2021*, para. 34.

[113] Domenig/Mitscherlich/Lutz, 'Datenschutzrecht für Schweizer Unternehmen, Stiftungen und Vereine', para. 485; Rosenthal, 'Löschen und doch nicht löschen', 192; Apollo Dauag/Liliane Obrecht, 'Art. 32 SDPA', in Adrian Bieri/Julian Powell (eds), *DSG, Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen* (Zurich: Orell Füssli, 2023) paras. 46 f; Philipp Glass, 'Art. 5 SDPA', in Adrian Bieri/Julian Powell (eds), *DSG, Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen* (Zurich: Orell Füssli, 2023), paras. 8 ff.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

(be it the destruction of the data medium or the other types of physical erasure) while that of erasure refers to a surprisingly liberal perspective which is limited to ordinary deletion (see definition cf. *supra* I. B).

IV. Conclusions

A. Synthesis

European and Swiss law have some common features in terms of legal policy which leads to the risk of significant technological biases.

Both the GDPR and the SDPA are drafted from a technology-neutral perspective. The principle of technological neutrality is not a legal principle strictly speaking but merely a way to approach the design of legislative texts in order to avoid, a priori, that some technologies may be excluded from their scope of application.[114] Although this principle guides the drafting of the legal text, it does not as such prevent specific rules to be enacted a posteriori.[115] While laudable in principle, such a policy-making choice must have its advantages and drawbacks carefully weighed. On the one hand, an inherent feature of the technology-agnostic approach is to leave a broad freedom of interpretation and implementation with the idea of allowing adjustments to future technical innovations.[116] It allows for the possibility to refer to technical standards. On the other hand, technological neutrality has the disadvantage that it does not allow the law to be specific about the subject matter which it regulates.[117]

In the digital area, drafting laws while ignoring the singularity of the nature of information under the guise of technological neutrality opens the door to technological bias. Regarding data erasure in particular, we have pointed out that handling digital data and paper data in similar ways can be at times limited and at worst counterproductive.

Echoing the considerations presented in Fig. 1 in the introduction, one can first observe that there is a high incentive for data controllers to keep the digital data they have under custody and never dispose of it (see storage and retrieval in Fig. 1) while

[114] Michael Montavon, 'L'abandon de la procédure d'appel en protection des données' (2020) *LeGes – Législation & Évaluation*, para. 12; Alexandre Barbey, 'Les lois dites technologiquement neutres face à la sécurité juridique', in Florence Guillaume (ed.), *La technologie, l'humain et le droit* (Bern: Staempfli, 2023), 7.

[115] Montavon, 'L'abandon de la procédure d'appel en protection des données', para. 12.

[116] Politou/Alepis/Patsakis, 'Forgetting personal data', 11.

[117] Chris Reed, 'Taking Sides on Technology Neutrality' (2007) *Script* 264.

University of Vienna Law Review, Vol. 9 No 3 (2025), pp. 64-98, https://doi.org/10.25365/vlr-2025-9-3-64.

the relatively extreme ease of copying and transporting digital data makes it relatively easy to circumvent erasure mandates.

Expanding on the processing that can be done and is done with digital data and is not done with analog data, we identify a bias towards underestimating data recovery techniques and how such techniques might improve in the future. This can therefore make the uninitiated practitioner unaware of the subtleties that lie at the boundary between reversible operations and irreversible erasure. Furthermore, the relative difficulty of actually implementing and then proving erasure of digital data when compared to analog data induces a bias towards the irreversible approach presented cf. *supra* II. C. 1. as opposed to the proportionate approach presented cf. *supra* II. C. 2. Irreversibility is in theory highly desirable but given the identified pitfalls in the digital domain, it is way more practical to favor the proportionate approach provided that the legal framework is grounded in the technical reality.

So far, these fundamental differences between the analog and digital realms have not been embraced by data protection laws. While Art. 17 (2) GDPR shyly tries to clarify the implementation of the right to be forgotten (and therefore not that of erasure *stricto sensu* itself) in the digital context when the controller has made the personal data public[118], the Swiss legislator on its side refrained from adding specific provisions even in the latest revision. Current laws are thus characterized by the (almost) total absence of domain-specific considerations.

Moreover, as a consequence of the technologically neutral approach, the legal texts neither define what erasure means nor which methods should be used. It is therefore to the data protection authorities to set the requirements for an efficient erasure while it belongs to the data controllers to choose the erasing methods, they deem adequate.[119] This puts a lot of pressure on the latter in terms of compliance.

An analysis of the practices developed by data protection authorities as well as opinions of legal scholars throughout the European Union shows that the approaches are quite varied and usually cover a wide range of methods (often mixing the irreversible and proportionate approaches). This broad approach leads to the existence of two competing views which constitute a genuine practical and intellectual dissent. There is however a growing trend towards the proportionate approach which is certainly due to the need to adapt to the current material and technical reality.

[118] However, this provision relates more to the right to be forgotten and is therefore out of scope as set out in footnote 13.

[119] Sven Hunzinger, 'Das Löschen im Datenschutzrecht', 64.

In contrast, it seems that in Swiss law, the notion of destruction keeps the meaning it had under the fSDPA, while that of erasure refers to ordinary deletion.

B. Authors' Opinions

The general trend toward the proportionate approach in European law is pragmatic from the technical point of view. Such an approach should therefore be favored, even if it is not sufficient to resolve all the legal uncertainty involved on its own. Some adjustments are advisable in order to avoid some of the identified pitfalls.

Swiss law is at a turning point. The SDPA completely leaves out the proportionate approach to erasure as it was developed in European law. This surprisingly liberal approach creates a definite risk in terms of security and privacy, and may jeopardize the protection of data subjects.

In our opinion, erasure should be understood as referring to the proportionate approach and exclude ordinary deletion. There are several advantages to this. First, it would fit the legislator's intention to better align the SDPA on the GDPR. Second, it would allow for the practice to take into account technical implementation imperatives. This could be carried out, for instance, by applying the right to destruction to paper documents while reserving the right to erasure for digital data, since erasure better fits the fundamental constraints of digital data. We therefore recommend that the actors adopt the proportionate approach and hope that such an approach will be, furthermore, favored by court decisions.

More generally, there is a dire need to recognize the added complexity of legislative tasks due to technological biases when it comes to data erasure and digital law more broadly. In the digital domain, the potential for technological bias stemming from technical misunderstanding seems higher than in other sectors. It is therefore imperative to adopt an even more rigorous legal approach, and to recognize that the legislative task associated with digital technology is all the more complex and requires a diligent consideration of domain-specific knowledge. Technological neutrality is a reasonable default in law-making, but it has to be weighed against the risk of making ineffective laws. For example, thinking of digital data as similar enough to data on paper, makes for a wrong mental framework which in turn gives rise to laws and regulations that are easy to circumvent.

Discussing potential solutions to this situation is a deep and nuanced topic that goes beyond the scope of this contribution. Any worthwhile effort to legislate in the field of digital law needs to be grounded in technical considerations. This task cannot be

left to legal experts alone as they lack the necessary domain-specific expertise and thus interdisciplinary cooperation may be more needed than ever.

V. Bibliography

A. Primary Sources

Administrative Court of Karlsruhe (*Verwaltungsgericht Karlsruhe*), decision 2 K 3249/12 of 27 May 2013 (2013) *Neue Zeitschrift für Verwaltungsrecht Rechtsprechungs-Report* 797

Austrian Data Protection Authority (*Österreichische Datenschutzbehörde*), decision DSB-D123.270/0009-DSB/2018 of 5 December 2018

Austrian Supreme Court (*Österreichischer Oberster Gerichtshof*), decision 6 Ob 41/10p of 15 April 2010 (2011) *Multimedia und Recht* 204

German Parliament (*Bundestag*), 'Draft Act of 24 February 2017 on the Adaptation of Data Protection Law to Regulation (EU) 2016/679 and the Implementation of Directive (EU) 2016/680, Document 18/11325' (*Deutscher Bundestag, Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, Drucksache 18/11325, 24. Februar 2017*)

State Social Court of Bayern (*Bayerisches Landessozialgericht*), decision L 15 SB 80/06 of 31 March 2011 (2011) *Beck-Rechtsprechung* 75017

Swiss Federal Administrative Court (*Bundesverwaltungsgericht*), decision BVGE 2015/13 of 23 April 2015

Swiss Federal Council, 'Message of 23 March 1988 on the Swiss Data Protection Act', Federal Gazette 1988 413 (*Schweizer Bundesrat, Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988', Bundesblatt (BBl) 1988 II 413*)

Swiss Federal Council, 'Message of 15 September 2017 on the Federal Act on the total revision of the Federal Data Protection Act and on the amendment of other federal acts, Federal Gazette 2017 6565' (*Schweizer Bundesrat, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, Bundesblatt (BBl) 2017 6565*)

B. Secondary Sources

Marian Alexander Arning, 'Art. 17 GDPR', in Flemming Moos/Jens Schefzig/Marian Alexander Arning (eds), *Praxishandbuch DSGVO* (Frankfurt am Main: Recht und Wirtschaft, 2021)

Marian Alexander Arning, in Flemming Moos/Jens Schefzig/Marian Arning (eds), 'Die neue Datenschutz-Grundverordnung' (Berlin: De Gruyter, 2018)

Manos Athanassoulis/Subhadeep Sarkar/Tarikul Islam Papon/Zichen Zhu/Dimitris Staratzis, 'Building Deletion-Compliant Data Systems' (2022) *Institute of Electrical and Electronics Engineers Data Engineering Bulletin* 21

Jef Ausloos, 'The Right to Erasure in EU Data Protection Law, From Individual Rights to Effective Protection' (Oxford: University Press, 2020)

Alexandre Barbey, 'Les lois dites technologiquement neutres face à la sécurité juridique', in Florence Guillaume (ed.), *La technologie, l'humain et le droit* (Bern : Staempfli, 2023)

Cesare Bartolini/Lawrence Siry, 'The right to be forgotten in the light of the consent of the data subject' (2016) *Computer Law & Security Review* 218

Hans Bättig, 'Art. 21 fSDPA', in Urs Maurer-Lambrou/Nedim Peter Vogt (eds), *Kommentar zum schweizerischen Datenschutzgesetz* (Basel: Helbing Lichtenhahn, 1995)

Gabor-Paul Blechta, 'Art. 3 fSDPA' in Urs Maurer-Lambrou/Gabor-Paul Blechta (eds), *Datenschutzgesetz/Öffentlichkeitsgesetz* (Basel: Helbing Lichtenhahn, 2014)

François Bohnet, 'Actions civiles', Volume 1 (Basel: Helbing Lichtenhahn, 2019)

Malin Bradley/Latanya Sweeney, 'How (not) to protect genomic data privacy in a distributed network: using trail reidentification to evaluate and design anonymity protection systems' (2004) *Journal of Biomedical Informatics* 179

Robert Bühler, 'Art. 21 fSDPA' in Urs Maurer-Lambrou/Gabor-Paul Blechta (eds), *Datenschutzgesetz/Öffentlichkeitsgesetz* (Basel: Helbing Lichtenhahn, 2014)

Eva Cellina, 'La commercialisation des données personnelles' (Geneva: Schulthess, 2020)

Danish Data Protection Authority of September 2014, 'Guidelines to Personal Data Erasure' (*Datatilsynet, It-sikkerhedstekst ST3, Sletning af personoplysninger, September 2014*)

Data Protection Commissioner of the German State of Bavaria, 'Guidelines to the Right to Erasure of 1 June 2022' (*Der Bayerische Landesbeauftragte für den Datenschutz, Das Recht auf Löschung nach der Datenschutz-Grundverordnung, Orientierungshilfe, 1. Juni 2022*)

Data Protection Commissioner of the German State of Mecklenburg-Vorpommern, 'Module 60 "Erasure and Destruction" of 2 September 2020' (*Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Standard-Datenschutzmodell, Baustein 60 "Löschen und Vernichten" (Version 1.0a vom 2 September 2020*)

Data Protection Commissioner of the German State of Sachsen, '10th Activity Report of 1 September 2011' (*Landesbeauftragter für den Datenschutz Sachsen, X. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz, 1. September 2011*)

Apollo Dauag/Liliane Obrecht, 'Art. 32 SDPA', in Adrian Bieri/Julian Powell (eds), *DSG, Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen* (Zurich : Orell Füssli, 2023)

Wolfgang Däubler, 'Art. 17 GDPR', in Wolfgang Däubler/Peter Wedde/Thilo Weichert/Imke Sommer (eds), *EU-DSGVO und BDSG* (Frankfurt am Main: Bundes-Verlag, 2020)

Alexander Dix, 'Art. 17 GDPR', in Spiros Simitis/Gerrit Hornung/Indra Spiecker (eds), *Datenschutzrecht, DS-GVO mit BDSG* (Baden-Baden: Nomos, 2019)

Benjamin Domenig/Christian Mitscherlich/Chantal Lutz, 'Datenschutzrecht für Schweizer Unternehmen, Stiftungen und Vereine' (Bern: Staempfli, 2022)

Tilman M. Dralle, 'Recht auf Löschung: der Radiergummi der DS-GVO' (2017) *Berufsverband der Datenschutzbeauftragten Deutschlands-NEWS (BvD-NEWS)* 47

Matthias Enzmann/Annika Selzer/Dominik Spychalski, 'Data Erasure under the GDPR – Steps towards Compliance' (2019) *European Data Protection Law Review (EDPL)* 416

Marco Fey, 'Art. 21', in Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (eds), *Datenschutzgesetz* (Bern: Staempfli, 2015)

Armin Fladung, 'Art. 17 GDPR', in Tim Wybitul (ed.), *Handbuch EU-Datenschutz-Grundverordnung* (Frankfurt am Main: Recht und Wirtschaft, 2017)

Eva Gardyan-Eisenlohr/Cay Lennart Cornelius, 'Datenlöschung', in Flemming Moos/Jens Schefzig/Marian Alexander Arning (eds), *Praxishandbuch DSGVO* (Frankfurt am Main: Recht und Wirtschaft, 2021)

Philipp Glass, 'Art. 5 SDPA', in Adrian Bieri/Julian Powell (eds), *DSG, Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen* (Zurich : Orell Füssli, 2023)

Niko Härting, 'Datenschutz-Grundverordnung' (Köln: Dr. Otto Schmidt, 2016)

Tobias Herbst, 'Art. 17 GDPR', in Jürgen Kühling/Benedikt Buchner, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Kommentar (Munich: C.H Beck, 2020)

Sven Hunzinger, 'Das Löschen im Datenschutzrecht' (Frankfurt: Nomos, 2018)

Sandra Husi-Stämpfli, 'Entstehungsgeschichte' in Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (eds), *Datenschutzgesetz* (Bern: Staempfli, 2023)

Irish Data Protection Commission, 'Guidance Note: Guidance for Controllers on Data Security of February 2020'

Emilie Jacot-Guillarmod, 'Art. 5 SDPA', *in* Yaniv Benhamou/Bertil Cottier, *Loi fédérale sur la protection des données* (Basel : Helbing Lichtenhahn, 2023)

Dietmar Jahnel, 'Art. 17 GDPR', in Dietmar Jahnel/Christian Bergauer (eds), *Kommentar zum DSGVO* (Wien: Jan Sramek, 2021)

Yvonne Jöhri, 'Art. 21 fSDPA' in David Rosenthal/Yvonne Jöhri (eds), *Handkommentar zum Datenschutzgesetz* (Basel/Geneva: Schulthess, 2008)

Nikolai Joukov/Harry Papaxenopoulos/Erez Zado, 'Secure Deletion Myths, Issues, and Solutions' (2006) *Proceedings of the second Association for Computing Machinery workshop on Storage security and survivability* 61

Wulf Kamlah, 'Art. 17 GDPR', in Kai-Uwe Plath (ed.), *DSGVO/BDSG/TTDSG, Kommentar* (Köln: Dr. Otto Schmidt, 2023)

Marnie Kiener, 'Datenlöschung einer Bank im Lichte der Datenschutzgesetzgebung Schweiz und EU' (Zurich: Schulthess, 2023)

Sascha Kremer, 'Art. 17 GDPR', in Philipp Laue/Sascha Kremer (eds), *Das neue Datenschutzrecht in der betrieblichen Praxis* (Baden-Baden: Nomos, 2019)

Sabine Leutheusser-Schnarrenberger, 'Art. 17 GDPR', in Rolf Schwartmann/Andreas Jaspers/Gregor Thüsing/Dieter Kugelmann, *DS-GVO/BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (Heidelberg: C.F Müller Verlag, 2020)

Christina-Maria Leeb/Luisa Lorenz, 'Datenschutzkonforme Dokumentenentsorgung' (2018) *Zeitschrift für Datenschutz (ZD)* 573

Viktor Mayer-Schönberger, 'Delete, The Virtue of Forgetting in the Digital Age' (Princeton: University Press, 2011)

Philippe Meier/Nicolas Tschumy 'Art. 5 SDPA', in Philippe Meier/Sylvain Métille (eds), *Loi fédérale sur la protection des données* (Basel: Helbing Lichtenhahn, 2023)

Philippe Meier, 'Protection des données' (Bern: Staempfli, 2010)

Jan Geert Meents/Britta Hinzpeter, 'Art. 17 GDPR', in Jürgen Taeger/Detlev Gabel (eds), *DSGVO – BDSG – TTDSG, Kommentar* (Frankfurt am Main: Recht und Wirtschaft, 2022)

Sylvain Métille, 'La (nouvelle) loi fédérale sur la protection des données du 25 septembre 2020', in Astrid Epiney/Sophie Moser/Sophia Rovelli (eds), *La Révision de la Loi fédérale sur la protection des données* (Zurich: Schulthess, 2022)

Michael Montavon, 'Cyberadministration et protection des données, Etude théorique et pratique de la transition numérique en Suisse du point de vue de l'Etat, des citoyen-ne-s et des autorités de contrôle' (Geneva/Zurich/Basel: Schulthess, 2021)

Michael Montavon, 'L'abandon de la procédure d'appel en protection des données' (2020) *LeGes – Législation & Évaluation*

Arvind Narayanan/Vitaly Shmatikov, 'Robust De-anonymization of Large Sparse Datasets' (2008) *Institute of Electrical and Electronics Engineers (IEEE) Symposium on Security and Privacy* 111

Boris P. Paal, 'Art. 17 GDPR', in Boris P. Paal/Danuel A. Pauly, *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Beck'sche Kompakt-Kommentare* (Munich: C.H Beck, 2018)

Enrico Peuker, 'Art. 17 GDPR', in Gernot Sydow/Nikolaus Marsch (eds), *Datenschutz-Grundverordnung / Bundesdatenschutzgesetz, Handkommentar* (Baden-Baden: Nomos, 2022)

Eugenia Politou/Efthimios Alepis/Constantinos Patsakis, 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions' (2018) *Journal of Cybersecurity* 1

Chris Reed, 'Taking Sides on Technology Neutrality' (2007) *Script* 264

David Rosenthal, 'Art. 3 fSDPA', in David Rosenthal/Yvonne Jöhri (eds), *Handkommentar zum Datenschutzgesetz* (Geneva/Basel/Zurich: Schulthess, 2008)

David Rosenthal, 'Löschen und doch nicht löschen' (2019) *Digma* 190

David Rosenthal/Samira Studer/Alexandre Lombard, 'La nouvelle loi sur la protection des données' (2021) *Jusletter of 12 April 2021*

Alexander Roßnagel, 'Datenlöschung und Anonymisierung' (2021) *Zeitschrift für Datenschutz (ZD)* 188

Beat Rudin, 'Art. 5 SDPA', in Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (eds), *Datenschutzgesetz* (Bern: Staempfli, 2023)

Beat Rudin, 'Art. 3 fSDPA', in Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (eds), *Datenschutzgesetz* (Bern: Staempfli, 2015)

Peter W. Shor, 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer' (1997) *SIAM Journal on Scientific and Statistical Computing* 1484

Verena Stürmer, 'Löschen durch Anonymisieren? Mögliche Erfüllung der Löschpflicht nach Art. 17 DS-GVO' (2020) *Zeitschrift für Datenschutz (ZD)* 626

Oliver Stutz, '8. Datenlöschung', in Uwe Schläger/Jan-Christoph Thode (eds), Handbuch Datenschutz und IT-Sicherheit (Berlin: Erich Schmidt Verlag, 2022)

Latanya Sweeney, 'Weaving Technology and Policy Together to Maintain Confidentiality' (1997) *Journal of Law, Medicine & Ethics* 98

Herman T. Tavani, 'Informational Privacy: Concepts, Theories, and Controversies', in Kenneth E. Himma/Herman T. Tavani (eds), *The Handbook of Information and Computer Ethics* (Hoboken: John Wiley & Sons, 2008)

Luke Tredinnick, 'Digital Information Culture: The individual and the society in the digital age' (Oxford: Chandos Publishing, 2006)

Martin Winterberger-Yang, 'Art. 21 fSDPA', in Urs Maurer-Lambrou/Nedim Peter Vogt (eds), *Datenschutzgesetz* (Basel: Helbing Lichtenhahn, 2006)

Christoph Worms, 'Art. 17 GDPR', in Heinrich Amadeus Wolff/Stefan Brink (eds), *Datenschutzrecht, Kommentar* (Munich: C.H Beck, 2022)