Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 15, NUMBER 3 >>> MARCH 2015

Data Disposal Security Requirements under EU, Austrian and German Law

By Lukas Feiler and Holger Lutz, of Baker & McKenzie.

There are numerous "data disposal laws" in the United States that expressly address the question of how to securely dispose of personal data. In the European Union, the issue has, so far, not received the same level of attention.

In Austria, the issue of secure data disposal is discussed more broadly only since August 2014, when it was publicly reported that the Regional Criminal Court Vienna regularly disposed of paper copies of court files concerning ongoing proceedings in publicly accessible dumpsters.[1] This allowed a blogger to obtain, and subsequently report about,[2] the contents of numerous files from ongoing criminal proceedings using "dumpster diving."[3]

Incidents are also regularly reported where private corporations or government authorities sold their old computer hardware (*e.g.*, via eBay) without having properly deleted the personal data stored on such hardware.[4] For example, in September 2014 it was reported that the hard disk of an Austrian doctor's office containing unencrypted patient data was sold on eBay.[5]

This Special Report examines the extent to which the implementation of security measures during the data disposal process is required under the EU Data Protection Directive, Austrian law and German law. The Special Report concludes with a comparative analysis of U.S. law.

Mandatory Data Disposal under the EU Data Protection Directive

The EU Data Protection Directive[6] (hereinafter "EU DPD") does not expressly contain any data disposal requirements. However, it has to be considered that the erasure or destruction of personal data as well as the dissemination or otherwise making available of personal data constitutes a form of processing under Article 2(b) EU DPD[7] and therefore falls within the scope of the EU DPD. Moreover, Article 17 EU DPD provides that "the controller must implement appropriate technical and organizational measures to protect personal data against . . . unauthorized disclosure or access." In order to avoid unlawfully making available personal data and to comply with the requirements under Article 17 EU DPD, it is necessary to

implement appropriate security measures for the disposal of personal data.[8]

The EU Data Protection Directive does not expressly contain any data disposal requirements. However, in order to avoid unlawfully making available personal data and to comply with the requirements under Article 17 of the Directive, it is necessary to implement appropriate security measures for the disposal of personal data.

This applies to the extent that the processing in question falls within the material scope of application of the EU DPD which is defined in Article 3 EU DPD. Specifically, the EU DPD applies to the processing of personal data if 1) the processing is at least partly automated or 2) the data forms or is intended to form part of a "filing system."[9]

To determine whether the EU DPD applies to the disposal of manually processed data (*i.e.,* paper documents of any kind), it is essential to determine whether such data is (or is intended to be) part of a filing system. A filing system is defined as "any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis."[10]

Recital 27 EU DPD further explains that the definition of a filing system requires that its content is "structured according to specific criteria relating to individuals allowing easy access to the personal data." The legislative history provides that this structuring and access criteria must have "the 'object or effect' of facilitating the use or comparison of data."[11] However, instead of providing further guidance on the exact requirements of such criteria, Recital 27 EU DPD provides that "different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each EU Member State," thereby giving EU Member States the power to define the exact limits of the EU DPD's material scope of application as regards the manual processing of personal data.[12]

Whether manual files such as 1) those commonly produced by courts and administrative authorities as part of a judicial or administrative proceeding or 2) employee files fall within the scope of data protection law is therefore up to each EU Member State to decide. So, too, is the question whether there are any data disposal requirements for such manual files. Recital 27 reflects this legal uncertainty by stating that "files or sets of files as well as their cover pages, *which are not structured according to specific criteria*, shall under no circumstances fall within the scope of this Directive."[13]

Data Disposal Requirements under Austrian Law

Data Protection Law

The material scope of application of the federal Austrian Data Protection Act 2000[14] (hereinafter "Austrian DPA") covers 1) the protection of personal data that is automatically processed[15] and 2) manually processed structured sets of personal data which are accessible according to at least one specific criterion ("manual filing systems" as defined in § 4(6) Austrian DPA) if they exist for such purposes and fields where the Austrian federal government has the power to pass laws (§§ 4(6), 58 Austrian DPA).[16]

Pursuant to the catch-all clause of Article 15(1) of the Austrian Constitution,[17] all legislative competences not allocated otherwise rest with the nine Austrian provinces (Länder). This applies to 1) the protection of manually processed data that is not part of a filing system and 2) the protection of manual filing systems to the extent that they exist for such purposes and fields where the Austrian Länder have the power to pass laws.[18]

Given that the protection of only manual filing systems — but not of any other manually processed data — was mandatory to implement under the EU DPD,[19] all Länder have adopted data protection acts that are limited to manual filing systems.[20]

Manually processed data that is either 1) not structured or 2) not accessible according to at least one specific criterion is therefore not covered by any Austrian data protection statute.[21] The Austrian Supreme Court,[22] the Austrian Administrative Court,[23] the Austrian Constitutional Court,[24] and the Austrian Data Protection Authority[25] have all held that regular paper files — for example, court files or personnel files — are not a "filing system" and are therefore not subject to the Austrian DPA or to the data protection acts of the Länder.

An interim finding therefore is that the disposal of individual paper files or paper documents from such files is not subject to any requirements under Austrian data protection law.

In the following, the mandatory data disposal security measures that apply to all other types of personal data and are required under the Austrian DPA or the data protection acts of the Länder will be examined. These requirements under the Austrian DPA and the laws of the Länder are, in effect, identical, because all data protection laws of the Länder either refer to the Austrian DPA as regards at least data security requirements or reproduce the Austrian DPA's relevant provisions *verbatim.*[26]

§ 14(1) Austrian DPA requires the implementation of data security measures. These measures have to ensure *inter alia* that "the data . . . are not accessible to unauthorized persons."[27] To determine the necessary level of security, it first has to be considered what kind of data is used and to what extent and for which purposes the use is performed. This first element therefore refers to the risk associated with the data use. Secondly, the state of

   ISSN 1473-3579

technical possibilities and, thirdly, the economic justifiability have to be taken into account.

Moreover, even though the non-exhaustive list of mandatory security measures provided by § 14(2) Austrian DPA does not expressly refer to data disposal issues, it does nonetheless contain two requirements related to physical access control: Pursuant to § 14(2)(5) Austrian DPA, "the protection of storage media against access and use by unauthorized persons is to be regulated." Moreover, § 14(2)(6) Austrian DPA requires that "every device is . . . secured against unauthorized operation by taking precautions for the machines and programs used."[28] This makes clear that, at least for electronically processed data (the statute refers to "storage media" and "machines"), measures to secure the data disposal process are generally mandatory.

However, to determine the specific measures to be implemented in a given scenario, a risk-based approach has to be adopted.

On one end of the spectrum are legitimately published data and indirectly personal data which, if compromised during the disposal process, do not result in any practically relevant risks.[29] Legitimately published data are already available to the general public, and indirectly personal data (as defined in § 4(1) Austrian DPA) relate to the data subject in such a manner that the data recipients cannot establish the identity of the data subject by legal means. Therefore, in these cases (*e.g.,* copies of publicly available documents), there is generally no obligation to implement any measures to secure the data disposal process.

At the other end of the spectrum is sensitive data[30] which, if compromised, can result in very significant risks for the data subject. When disposing of a manual filing system or parts thereof, it is therefore generally required to shred or burn the documents. As regards electronic sensitive data, degaussing or physical destruction of the data carrier or the overwriting of data should be considered as primary disposal methods.[31]

To dispose of data by overwriting it, special-purpose software should be used that overwrites the data in question multiple times using different data sets.[32] Although such multi-pass overwriting is still considered as state of the art by many,[33] it is, indeed, possible to restore data disposed of in such manner if sufficient resources are put to the task. For that reason, U.S. Department of Defense standard DoD 5220.22-M,[34] which is often cited as a guideline for disposing of data by overwriting it,[35] was supplemented as early as 2007 to require the use of more secure disposal methods.[36] If the sensitive data in question is associated with a particularly high risk, the overwriting of data should therefore not be considered sufficient.

The simple deletion of an electronic file containing sensitive data is not adequate in any case, because the deletion of the file results only in the removal of the reference to the data carrier's physical storage areas in which the file contents are held. Thus, the content of the file (the sensitive data) remains fully intact and can be restored easily with special-purpose software.[37]

Austrian data protection law requires the implementation of risk-based security measures for the disposal of electronic data and manual filing systems. Manually processed data that is not part of a filing system, on the other hand, is not subject to any data protection and, in particular, is not the subject of any data disposal security requirements resulting from data protection laws.

So-called crime-related data[38] enjoys an overall level of protection under the Austrian DPA that is close to that of sensitive data. Such data should therefore generally be disposed of using the same process employed for sensitive data (*i.e.,* degaussing, physical destruction, or multi-pass overwriting in the case of electronic data, or shredding or burning in the case of filing systems). To dispose of crime-related data (that is part of a manual filing system) in a dumpster is therefore impermissible, irrespective of whether such dumpster is accessible from the street.

In the case of any other types of personal data, the simple deletion of the data files or a quick formatting of the hard drive could be sufficient if the risk presented is low. However, if there is any doubt, the data should be overwritten at least once (or a normal formatting of the data carrier should be performed which also results in the overwriting of all storage areas). As regards manual filing systems, a simple disposal in a dumpster may be sufficient in low-risk scenarios. If there is any doubt, it should be made sure that the dumpster is not publicly accessible.

In summary, Austrian data protection law requires the implementation of risk-based security measures for the disposal of electronic data and manual filing systems. Manually processed data that is not part of a filing system, on the other hand, is not subject to any data protection and, in particular, is not the subject of any data disposal security requirements resulting from data protection laws.

Rules of Professional Conduct and Sector-Specific Data Disposal Requirements

The protection deficit concerning manually processed data resulting from the limited material scope of application of Austrian data protection law is partly compensated by 1) rules of professional conduct of regulated professions and 2) sector-specific requirements.

In particular from the professional secrecy obligations of physicians,[39] tax advisors and chartered accountants,[40] notaries,[41] and attorneys,[42] it is possible to derive an obligation to prevent any third parties from gaining knowledge of any of the information subject to professional secrecy. In contrast to the obligations under data

protection law, this applies irrespective of whether electronic data, manual filing systems, or other manually processed data is concerned. In order to comply with these professional regulatory requirements, it is necessary to provide a particularly high level of security for the data disposal process. Therefore, in effect, the same level of security will have to be implemented as for sensitive data under § 14 Austrian DPA (as discussed above).

The protection of bank secrecy (§ 38 Austrian Banking Act[43]) and telecommunications secrecy (§ 93 Austrian Telecommunications Act 2003[44]) also requires similarly strict data disposal security measures. These requirements, too, apply irrespective of whether electronic data, manual filing systems, or other manually processed data is concerned.

Data Disposal Requirements under German Law

Data Protection Law

With regard to the processing of personal data by private bodies,[45] the material scope of the German Federal Data Protection Act[46] (hereinafter "German FDPA") generally covers the protection of personal data that is 1) processed or used in data processing systems (or collected for such systems) and 2) processed or used in or from non-automated filing systems (or collected for such systems), unless the data are collected, processed or used solely for personal or domestic activities (§ 1(2) German FDPA).

Similar to the situation under Austrian law, manually processed data that is either 1) not structured or 2) not accessible according to at least one specific criterion is therefore not covered by the German FDPA. However, it should be noted that the German data protection authorities tend to apply a fairly low threshold for data being structured and accessible to specific criteria.

In addition, with regard to the collection, processing or use of personal employee data, the material scope of the German FDPA is broadened, and also covers the collection, processing and use of such data without the help of automated processing systems, or in or from a non-automated filing system (§ 32(2) German FDPA).[47]

Thus, an interim finding under German law is that the disposal of individual paper files or paper documents from such files is, in any case, subject to German data protection law if it relates to personal employee data, and is often subject to German data protection law if it relates to personal data other than personal employee data.

The mandatory data disposal security measures that apply to all types of personal data subject to the German FDPA are similar to the ones applicable in Austria.

§ 9 German FDPA requires the implementation of technical and organizational measures to ensure the implementation of the provisions of the German FDPA. This includes, *inter alia,* measures to 1) prevent unauthorized persons from gaining access to data processing systems for processing or using personal data;[48] 2) prevent data processing systems from being used without authorization;[49] 3) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording;[50] and 4) ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. This makes clear that, at least for electronically processed data, measures to secure the data disposal process are generally mandatory.

Pursuant to § 9 German FDPA, the respective measures are necessary only if the effort required is in reasonable proportion to the desired purpose of protection. In particular, the measures shall be suited to the type of personal data or categories of data to be protected.[51]

As under Austrian law, a risk-based approach must be taken to determine the specific measures to be implemented in a given scenario. The more sensitive the relevant data and the higher the number of affected data subjects, the higher the requirements to secure the data disposal process. With regard to the different means to dispose of personal data, the German data protection authorities refer to certain security standards as defined in Deutsches Institut für Normung ("DIN") (German Institute for Standardization) standards[52] that define the condition, form and size of the material after disposal.

In summary, German data protection law requires the implementation of risk-based security measures for the disposal of personal data. Only in exceptional cases, manually processed data that is 1) not structured or 2) not accessible according to at least one specific criterion is — to the extent it is not personal employee data — not subject to any data protection and, in particular, not the subject of any data disposal security requirements under data protection law.

Rules of Professional Conduct and Sector-Specific Data Disposal Requirements

In addition to the protection under German data protection law, additional disposal security requirements can be derived from 1) rules of professional conduct of regulated professions and 2) sector-specific requirements. Similar to Austrian law, such obligations can be derived in particular from professional secrecy obligations of physicians, professional psychologists, attorneys, notaries, public accountants, members of health, accident or life insurance companies and tax consultants (§ 203(1) German Criminal Code) containing an obligation to prevent any third parties from gaining knowledge of any of the information subject to professional secrecy.

   ISSN 1473-3579

German data protection law requires the implementation of risk-based security measures for the disposal of personal data. Only in exceptional cases, manually processed data that is 1) not structured or 2) not accessible according to at least one specific criterion is — to the extent it is not personal employee data — not subject to any data protection and, in particular, not the subject of any data disposal security requirements under data protection law.

In contrast to the obligations under data protection law, the respective obligations apply irrespective of whether electronic data, manual filing systems, or other manually processed data is concerned. In order to comply with these professional regulatory requirements, it is necessary to provide a particularly high level of security for the data disposal process. In most cases, a disposal should at least comply with level 4 of the security standards set out in DIN 32 757 (01/1995) and DIN 33 858 (04/1993).

The protection of bank secrecy and telecommunications secrecy (§ 88 German Telecommunications Act) also requires similarly strict data disposal security measures. These requirements, too, apply irrespective of whether electronic data, manual filing systems, or other manually processed data is concerned.

A Comparative Analysis of U.S. Law

Data disposal requirements that expressly mandate certain security measures when disposing of data exist under U.S. federal law as well as U.S. state law.

On the federal level, the Federal Trade Commission ("FTC"), the Securities and Exchange Commission ("SEC"), the federal banking agencies[53] as well as the National Credit Union Administration ("NCUA") have issued regulations on the basis of § 628 of the Fair Credit Reporting Act[54] requiring, respectively, the implementation of "reasonable measures" to protect "consumer reports"[55] against unauthorized access or use in connection with their disposal.[56]

Additionally, 32 of the 50 states have adopted data disposal laws[57] with different scopes of application. For example, California adopted Assembly Bill 2246[58] as early as 2000, requiring the implementation of reasonable steps to dispose, or arrange for the disposal, of customer[59] records containing broadly defined "personal information"[60] by 1) shredding, 2) erasing, or 3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.[61]

The data disposal law in the State of New York, on the other hand, in effect applies only to personal information which, if compromised, would result in a risk of "identity theft" (also and more fittingly described as "impersonation fraud"[62]): any information in combination with: 1) a Social Security number; 2) driver's license number or non-driver identification card number; or 3) mother's maiden name, a number or code for a financial service, savings account, checking account, debit card, ATM, or an electronic serial number or personal identification number.[63] The disposal of any other personal data therefore does not require any security measures under New York state law.

U.S. law is therefore characterized by a sector-specific regulatory approach on the federal level and rather inhomogeneous legislation at the state level. However, the data disposal requirements under U.S. federal and state law have in common that they generally apply irrespective of whether electronic or manually processed data are concerned.[64] The above-described requirements under U.S. law therefore apply in particular if the data to be disposed of is manually processed data that is not part of a "filing system" (as defined under Article 2(c) EU DPD or § 4(6) Austrian DPA).

Summary

Austrian data protection law requires the implementation of risk-adequate security measures when disposing of personal data. However, given that Austrian data protection law does not apply to manually processed data that is not part of a "filing system" — such as individual paper files — there is a significant protection deficit, which is compensated only partly by rules of professional conduct for regulated professions and sector-specific regulations.

In distinction from Austrian data protection law, the scope of application of German data protection law is significantly broader. Consequently, the protection deficit that exists under German data protection law is significantly smaller than that under Austrian data protection law, and is, in most cases, compensated by rules of professional conduct and sector-specific regulations.

A comparison with the legal situation in the U.S. makes clear that extending data disposal security requirements to cover all manually processed data is, indeed, practical and, in light of the risks for the privacy of individuals, more than appropriate.

NOTES

[1] *See* Kurier, *Justizpanne: Blogger fand streng geheime Akten* [*Judicial Glitch: Blogger Found Strictly Confidential Files*], KURIER.AT (Austria), Aug. 27, 2014, http://kurier.at/wirtschaft/wirtschaftspolitik/justizpanne-blogger-fand-streng-geheime-akten/82.466.252.

[2] *See* Kurier, *Blogger will 'Meinl-Akte' im Altpapier gefunden haben* [*Blogger Claims to Have Found 'Meinl File' in Recycle Bin*], KURIER.AT (Austria), Aug. 27, 2014, http://kurier.at/wirtschaft/wirtschaftspolitik/blogger-will-meinl-akte-im-altpapier-gefunden-haben/82.415.914.

[3] *Cf. Johnny Long, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing* (2008).

[4] Der Spiegel, *IT-Firma versteigert Festplatte mit Millionen Kontodaten* [*IT Company Auctions off Hard Disk Containing Millions of Bank Account Records*], SPIEGEL ONLINE (F.R.G.), Aug. 26, 2008, *available at* http://www.spiegel.de/netzwelt/web/0,1518,574470,00.html; Stephen Mihm,

Dumpster-Diving for Your Identity, N.Y. TIMES, Dec. 21, 2003, *available at* http://www.nytimes.com/2003/12/21/magazine/dumpster-diving-for-your-identity.html?partner=rssnyt&emc=rss&pagewanted=1; Maureen Culley & Vanessa Allen, *New data blunder as details of thousands of council taxpayers are found on £6.99 computer sold on eBay*, DAILY MAIL (U.K.), Aug. 27, 2008, *available at* http://www.dailymail.co.uk/news/article-1049413/New-data-blunder-details-thousands-council-taxpayers-6-99-sold-eBay.html; Jessica Salter, *Camera sold on eBay contained MI6 files*, DAILY TELEGRAPH (U.K.), Sept. 30, 2008, available at http://www.telegraph.co.uk/news/uknews/3107003/Camera-sold-on-eBay-contained-MI6-files.html.

[5] Patrick Dax, *Patientendaten auf gebrauchter Festplatte gefunden* [*Patient Data Found on Used Hard Disk*], FUTUREZONE (Austria), Sept. 8, 2014, http://futurezone.at/digital-life/patientendaten-auf-gebrauchter-festplatte-gefunden/84.416.151.

[6] Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

[7] Article 2(b) EU DPD defines "processing" as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as . . . erasure or destruction."

[8] *Cf., e.g., Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE)*, Recital 25, 2010 O.J. (C 280) 16, 19.

[9] Article 3(1) EU DPD.

[10] Article 2(c) EU DPD.

[11] *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, at 10, COM(92) 422 final (Oct. 15, 1992). The cited paragraph is missing in the reprint in ULRICHT DAMMANN & SPIROS SIMITIS, EG-DATENSCHUTZRICHTLINIE [EC DATA PROTECTION DIRECTIVE] 107 (1997).

[12] *Cf. id.* at 111 (criticizing this approach as necessarily resulting in barriers to the free movement of manually processed personal data). *But see Eugen Ehmann & Marcus Helfrich, EG-Datenschutzrichtlinie* [EC DATA PROTECTION DIRECTIVE] (1999) Article 2 Recital 37 (stating that Recital 27 EU DPD would not leave EU Member States any room when implementing Article 2 EU DPD and that files or sets of files would, in any case, not fall within the scope of the EU DPD).

[13] Recital 27 EU DPD (emphasis added).

[14] Datenschutzgesetz 2000 [DSG 2000] [Austrian DPA] Bundesgesetzblatt [BGBl] I No 165/1999, as amended (Austria).

[15] § 2(1) Austrian DPA.

[16] Since the entry into force of the Data Protection Amendment Act 2010, BGBl I 133/2009, the Austrian DPA's scope of application, according to the plain language of the statute, seems to cover — in violation of the limited legislative competences of the Austrian Federal Government and contrary to the documented intent of the Austrian Parliament — any personal data, including all manually processed data. *Cf.* Daniel Ennöckl, *Die DSG-Novelle 2010* [*The Data Protection Amendment Act 2010*], 2010 OJZ 293, 293 *et seq.* (Austria); Daniel Ennöckl, *Die wesentlichen Neuerungen im DSG 2000* [The Material Amendments to the Austrian DPA] in DATENSCHUTZRECHT 2010 [DATA PROTECTION LAW 2010] 37, 43 (Nicolas Raschauer ed., 2011); VIKTOR MAYER-SCHONBERGER ET AL., DATENSCHUTZGESETZ [DATA PROTECTION ACT] 9 (3rd ed. 2014); WALTER DOHR ET AL., DSG [DATA PROTECTION ACT] § 4 Recital 7a (2nd ed.). Following the principle of a Constitution-compliant interpretation and considering §§ 12(1), 58 Austrian DPA within the framework of a systematic interpretation, a restrictive interpretation of the Austrian DPA is to be applied so that its scope of application can be brought into compliance with the limited legislative competences of the Austrian Federal Government.

[17] Bundes-Verfassungsgesetz [B-VG] [Constitution] BGBl No. 1/1930, as last amended by Bundesgesetz [BG] BGBl I No 102/2014 (Austria).

[18] *Cf.* Natalie Fercher, *Manuelle Dateien im Datenschutzgesetz 2000* [*Manual Filing Systems under the Austrian DPA*] in AKTUELLE FRAGEN DES DATENSCHUTZRECHTS [CONTEMPORARY QUESTIONS OF DATA PROTECTION LAW] 33, 37 (Dietmar Jahnel ed., 2007).

[19] Discussed under the section on the EU Data Protection Directive above.

[20] *See* Wiener Datenschutzgesetz [Viennese Data Protection Act], Landesgesetzblatt [LGBl] 125/2001 (hereinafter "VDPA"), § 2(1); Niederösterreichisches Datenschutzgesetz [Lower-Austrian Data Protection Act], LGBl 0901-0 Stammgesetz 116/00 2000-12-21 (hereinafter "LDPA"), § 2(1); Oberösterreichisches Auskunftspflicht-, Datenschutz- und Informationsweiterverwendungsgesetz [Upper-Austrian Freedom of Information, Data Protection, and Information Re-Use Act], LGBl 46/1988, as amended (hereinafter "UDPA"), § 8(2); Salzburger Gesetz über Auskunftspflicht, Dokumentenweiterverwendung, Datenschutz, Landesstatistik und Geodateninfrastruktur [Salzburg Freedom of Information, Document Re-Use, Data Protection, Local Statistics, and Geo Data Infrastructure Act], LGBl 3/1988 (hereinafter "SDPA"), § 20(2); Steiermärkisches Datenschutzgesetz [Styrian Data Protection Act], LGBl 39/2001 (hereinafter "StDPA"), § 2(1); Kärntner Informations- und Statistikgesetz [Carinthia Information and Statistics Act], LGBl 70/2005 (hereinafter "CDPA"), § 13(2); Tiroler Datenschutzgesetz 2014 [Tyrolean Data Protection Act 2014], LGBl 158/2013 (hereinafter "TDPA"), § 2(1); Vorarlberger Landes-Datenschutzgesetz, LGBl. 19/2000 as amended (hereinafter "VoDPA"), § 2 Abs 1; Burgenländisches Datenschutzgesetz [Burgenland Data Protection Act], LGBl 87/2005 as amended (hereinafter "BDPA"), § 2(1).

[21] Protection under fundamental rights does exist under § 1(1) Austrian DPA and Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter "ECHR"), Nov. 11, 1950, Council of Europe CETS No. 005, 213 U.N.T.S. 222 as well as — when implementing EU law — under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, 2007 O.J. (C 303) 1 (hereinafter "Charter"). *Cf.* Natalie Fercher, *Manuelle Dateien im Datenschutzgesetz 2000* [*Manual Filing Systems under the Austrian DPA*] in AKTUELLE FRAGEN DES DATENSCHUTZRECHTS [CONTEMPORARY QUESTIONS OF DATA PROTECTION LAW] 33, 40 *et seqq.* (Dietmar Jahnel ed., 2007). However, such fundamental rights protection does not result in any direct obligations for the administrative or judicial branches of the government or for corporations as regards the protection of such data in general and, specifically, data disposal.

[22] Oberster Gerichtshof [OGH] [Supreme Court] June 28, 2000, 6 Ob 148/00h (Austria); *cf. also* Claudia Rosenmayr-Klemenz, *Zum Schutz manuell verarbeiteter Daten durch das DSG 2000* [*On the Protection of Manually Processed Data by the Austrian DPA*], 2001 ECOLEX 639 (Austria).

[23] Verwaltungsgerichtshof [VwGH] [administrative court] Oct. 21, 2004, docket No. 2004/06/0086, Erkenntnisse und Beschlüsse des Verwaltungsgerichtshofes Administrativrechtlicher Teil [VwSlg] 16477 A (Austria).

[24] Verfassungsgerichtshof [VfGH] [Constitutional Court] Nov. 30, 2005, docket No. B1158/03, Erkenntnisse und Beschlüsse des Verfassungsgerichtshofes [VfSlg] No. 17.716 (Austria).

[25] Datenschutzkommission [DSK] [Data Protection Authority] Nov. 10, 2000, docket No. 120.707/7-DSK/00 (holding that administrative files are not "filing systems" because, although they are typically organized by a search term (the docket number), single files by themselves do not have a structured content; *cf.* also DSK Mar. 11, 2005, docket No. K120.969/0002-DSK/2005 (stating that commonly used administrative paper files are not filing systems unless additional structuring elements are present); DSK Oct. 11, 2005, docket No. K121.043/0008-DSK/2005.

[26] § 4(1) VDPA; § 14 LDPA; § 9(2) UDPA; § 21(2) SDPA; § 14 StDPA; § 14(3) CDPA; § 5 TDPA; § 4(1) VoDPA; § 13 BDPA.

[27] § 14(1) Austrian DPA.

[28] *Cf.* Dietmar Jahnel, *Datensicherheit und Datengeheimnis* [*Data Security and Data Secrecy*] in AKTUELLE FRAGEN DES DATENSCHUTZRECHTS [CONTEMPORARY QUESTIONS OF DATA PROTECTION LAW] 79, 87 *et seq.* (Dietmar Jahnel ed., 2007)

[29] *Cf.* § 8(2) Austrian DPA (stating that the use and processing of legitimately published data or indirectly personal data shall *per se* not constitute an infringement of the data subject's interests in secrecy deserving protection).

[30] *See* § 4(2) Austrian DPA (defining sensitive data as "[d]ata relating to natural persons concerning their racial or ethnic origin, political opinion, trade union membership, religious or philosophical beliefs, and data concerning health or sex life").

[31] As regards the possibility of restoring data that was improperly disposed of, *see generally* DAN FARMER & WIETSE VENEMA, FORENSIC DISCOVERY 145 (2004). *Cf. also U.S. National Institute of Standards and Technology, Guidelines for Media Sanitization, SP 800-88 Rev. 1* (2012), *available at* http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf.

   ISSN 1473-3579

[32] *E.g.,* the program "shred" for Linux/UNIX or the program "SDelete" which was developed by Mark Russinovich for the Windows operating system; *cf.* http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx; https://www.gnu.org/software/coreutils/manual/html_node/shred-invocation.html.

[33] *Cf., e.g., Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE),* Recital 31, 2010 O.J. (C 280) 16, 19.

[34] U.S. Department of Defense, National Industrial Security Program (NISP) Operating Manual, DoD 5220.22M (2006), *available at* http://www.dss.mil/documents/odaa/nispom2006-5220.pdf.

[35] *Cf. id.* at ch. 8, sec. 3, subsec. 8-301.

[36] U.S. Department of Defense, US Defense Security Service Clearing and Sanitization Matrix (2007), *available at* http://www.oregon.gov/DAS/OP/docs/policy/state/107-009-005_Exhibit_B.pdf.

[37] *See Dan Farmer & Wietse Venema, Forensic Discovery* 145 *et seqq.* (2004).

[38] *See* § 8(4) Austrian DPA (referring to "data concerning acts and omissions punishable by the courts or administrative authorities, and in particular concerning suspected criminal offenses, as well as data concerning criminal convictions and preventive measures [under criminal law]").

[39] Ärztegesetz 1998 [ÄrzteG 1998] [Physicians Act 1998], BGBl I No 169/1998, as amended, § 54 (Austria).

[40] Wirtschaftstreuhandberufsgesetz [WTBG] [Act on the Profession of Chartered Accountants], BGBl I No 58/1999, as amended, § 91 (Austria).

[41] Notariatsordnung [NO] [Act on Notaries] Reichtsgesetzblatt [RGBl] No. 75/1871, as amended, § 37 (Austria).

[42] Rechtsanwaltsordnung [RAO] [Act on Attorneys] RGBl No. 96/1868, as amended, § 9(2) (Austria).

[43] Bankwesengesetz [BWG] [Banking Act] BGBl I No. 532/1993, as amended (Austria).

[44] Telekommunikationsgesetz 2003 [TKG 2003] [Telecommunications Act 2003] BGBl I No 70/2003, as amended (Austria).

[45] The scope of application of the German FDPA is broader with regard to the collection, processing or use of personal data by public bodies (*cf.* § 1(2) German FDPA).

[46] Bundesdatenschutzgesetz [Federal Data Protection Act], Jan. 14, 2003, BGBl. I at 66, as amended (F.R.G.).

[47] This extension of the material scope of the German FDPA was implemented into German law in 2009 with effect as of Sept. 1, 2009.

[48] No. 1 of the Annex to § 9 German FDPA.

[49] No. 2 of the Annex to § 9 German FDPA.

[50] No. 3 of the Annex to § 9 German FDPA.

[51] Sent. 1 of the Annex to § 9 German FDPA.

[52] DIN 32 757 (01/1995) and DIN 33 858 (04/1993).

[53] These are the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("Board"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of Thrift Supervision ("OTS").

[54] Fair Credit Reporting Act, Pub. L. 91-508, 84 Stat. 1114 (1970) (codified as amended at 15 U.S.C. § 1681).

[55] *See* 15 U.S.C. § 1681a(d)(1) (defining "consumer report" as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under [15 U.S.C. § 1681b]").

[56] FTC Disposal Rule, 68 Fed. Reg. 68,690 (Nov. 24, 2004) (codified at 16 C.F.R. pt. 682); SEC Disposal Rule, 69 Fed. Reg. 71,322 (Dec. 8, 2004) (codified at 17 C.F.R. pt. 248); Interagency Disposal Rule, 69 Fed. Reg. 77610 (Dec. 28, 2004) (codified at 12 C.F.R. pts. 30 and 40 [OCC], 12 C.F.R. pts. 208, 211, 222, and 225 [Board], 12 C.F.R. pts. 334 and 364 [FDIC], 12 C.F.R. pts. 568, 570, and 571 [OTS]); NCUA Disposal Rule, 69 Fed. Reg. 69269 (Nov. 29, 2004) (codified at 12 C.F.R. pts. 717 and 748). *Cf. Lukas Feiler, Information Security Law in the EU and the U.S.* 84 *et seq.* (2011).

[57] See the list available on the website of the National Conference of State Legislatures at http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

[58] 2000 Cal. Adv. Legis. Serv. 5942 (Deering) (codified at Cal. Civ. Code §§ 1798.80-82).

[59] *See Cal. Civ. Code* §§ 1798.80(c) (West 2010) (defining "customer" as "an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business").

[60] *See Cal. Civ. Code* § 1798.80(e) (West 2010) (defining "personal information" broadly as "any information that identifies, relates to, describes, or is capable of being associated with, a particular individual," not including "publicly available information that is lawfully made available to the general public from federal, state, or local government records").

[61] *Cf. Lukas Feiler, Information Security Law in the EU and the U.S.* 103 (2011).

[62] *Cf. id.* at 116.

[63] N.Y. Gen. Bus. Law § 399-h(1)(d) (McKinney 2014).

[64] All data disposal regulations issued pursuant to Fair Credit Reporting Act § 628 expressly refer to "paper, electronic, or other form." *See* FTC Disposal Rule, 16 C.F.R. § 682.1(b); SEC Disposal Rule, 17 C.F.R. § 248.30(b)(1)(ii); Interagency Safeguards Guidelines I.C.2.b.; NCUA Disposal Rule, 12 C.F.R. § 717.83(d)(1). *See also Cal. Civ. Code* §§ 1798.80(b) (West 2010) (defining "records" as "any material, regardless of the physical form, on which information is recorded or preserved by any means"); N.Y. Gen. Bus. Law § 399-h(1)(b) (defining "record" as "any information kept, held, filed, produced or reproduced by, with or for a person or business entity, in any physical form whatsoever").

Dr. Lukas Feiler, Ph.D., SSCP, is an Associate at Baker & McKenzie, Vienna, and a Fellow of the Stanford-Vienna Transatlantic Technology Law Forum. He may be contacted at lukas.feiler@bakermckenzie.com.

Dr. Holger Lutz, LL.M., is a Partner at Baker & McKenzie, Frankfurt, and Co-Head of the Internet & eCommerce expert committee of the German Association of Law and Informatics (Deutsche Gesellschaft für Recht und Informatik e.V.). He may be contacted at holger.lutz@bakermckenzie.com.