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 14, NUMBER 3 >>> MARCH 2014

Big Data under Austrian Data Protection Law

By Lukas Feiler, of Baker & McKenzie, Vienna, and Prof. Siegfried Fina, of the University of Vienna School of Law.

The term "Big Data" refers to data quantities too large to be reasonably processed using conventional means of information technology (IT).[1] In most cases, Big Data consists of unstructured data (*e.g.,* business correspondence) which is insufficiently embodied in relational databases.[2]

However, the rapidly growing capacity of IT systems as well as new technologies for the processing of large amounts of data in memory (so-called In-Memory Computing) permit the implementation of complex data analysis processes suitable for Big Data. This makes it possible to derive new kinds of information from Big Data, such as future customer behavior, employee potential, or people's criminal intentions — all this under the caveat that such predictions are necessarily probabilistic inferences.[3]

Big Data in Conflict with Data Protection Principles

Pursuant to § 6(1)(2) of the Austrian Data Protection Act 2000 (hereinafter DPA),[4] personal data may be collected only for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. This codifies the principle of purpose limitation and, as its logical precondition, the principle of purpose specification.

In practice, for many Big Data applications, it is already difficult to achieve compatibility with the principle of purpose specification.[5] Due to the associated costs, in the past, data was generally retained only if it served a specific (economic) purpose. Today, the costs of data storage are so low that data is often collected and retained "just in case."[6]

When data stored in a Big Data application is to be processed for new purposes, the aforementioned principle of purpose limitation has to be observed. Therefore, a re-use is, in principle, permissible only for such new purposes which are compatible with the originally specified purposes.[7] For example, an incompatibility with the originally specified processing purposes exists if a controller's customer service requests which were previously processed only for quality control purposes are now also processed for marketing purposes.[8]

An exception from the principle of purpose limitation is provided by § 6(1)(2) DPA, which allows for further use for scientific and statistical purposes pursuant to §§ 46 and 47 DPA. Section 47 DPA concerns only the transmission of addresses to inform or interview data subjects, and is therefore of no practical relevance as regards Big Data. However, § 46 DPA is potentially relevant for the re-use of data in a Big Data application.

Big Data brings about a change not only in the quantity of the data processed but also in the quality of the processing itself.

Section 46 DPA covers exclusively the processing of data for the purposes of "scientific research" and "statistics" where both purposes are characterized by the application of scientific methods.[9] From this, two different statutory bases exist which allow data that was collected for different purposes to be re-used for research and statistics purposes:

First, such re-use is permissible without the authorization of the Austrian Data Protection Authority, if it is performed for the purpose of scientific or statistical "studies" which do not aim to produce any personalized results (§ 46(1) DPA).[10] According to the legislative history, the term "study" is limited to individualized research projects or individualized statistical surveys[11] and does not cover the permanent storage of personal data in the context of research and statistics.[12] Applied to Big Data, this means that only an isolated analysis of existing data for other purposes is covered by the term "study," whereas the permanent transfer of personal data into a Big Data application is not. Thus, in the context of Big Data, the first statutory basis provided by § 46 DPA is rarely relevant in practice.

The second statutory basis covers such processing of data for scientific research and statistical purposes which either 1) are studies that do have personalized results or 2) cannot be considered a "study" in the first place (§ 46(2) DPA).[13] On this statutory basis, unless the data processing is covered by a special statutory provision (§ 46(2)(1) DPA) or the data subjects' consent has been obtained (§ 46(2)(2) DPA), the re-use of data may occur only subject to the prior approval of the Austrian Data Protection Authority (§ 46(2)(3) DPA). According to § 46(3) DPA, such approval may be issued only if 1) obtaining the data subjects' consent is impossible or unreasonable, 2) a public interest exists in the re-use of the data, and 3) the data controller demonstrates its professional suitability. However, as regards private-sector controllers, a public interest in the re-use of data in a Big Data application is typically non-existent — the only exception being publicly funded research projects.[14]

As regards private-sector controllers of Big Data applications, the exceptions from the purpose limitation principle provided for by § 6(1)(2) in conjunction with § 46 DPA are therefore limited to the re-use of data for isolated research projects or isolated statistical surveys that do not aim to produce personalized results (*e.g.,* performing a statistical survey of the average customer's satisfaction with certain products of the company by a one-time analysis of customer correspondence).

However, if there is no exception from the principle of purpose limitation — which is commonly the case — any processing of data for a new purpose that is not compatible with the originally specified purposes constitutes, by legal definition, a transmission (§ 4(12) DPA).[15]

Pursuant to § 7(2) DPA, a transmission is permissible only if the legitimate interests of the data subjects are not infringed by the purpose and content of the transmission (§ 7(2)(3) DPA). For example, in cases where the legality of the original data processing was based on the data subject's consent pursuant to § 8(1)(2) DPA or a shop agreement pursuant to § 9(11) DPA, a new consent has to be obtained or a new shop agreement has to be concluded. This can be avoided only by drafting the original consent declaration or shop agreement with sufficient precision and with the necessary foresight.

Big Data Security under § 14 DPA

Section 14(1) DPA mandates that, for the purpose of maintaining data security, reasonable security controls are implemented, taking into account in particular "the kind of data used as well as the extent and purpose of the use." Ultimately, this requirement may also be described as reasonableness in light of the risk of an interference with the data subjects' rights.[16] The extent of the risk depends on the amount of potential damage as well as the probability that such damage will occur.[17]

Such a risk-based approach leads to the following considerations regarding the application of § 14 DPA to Big Data applications:

A Big Data application typically combines personal data that was previously processed on separate IT systems. Each of these separate IT systems ideally had security measures that corresponded to the risks associated with the respective data categories, and therefore complied with the requirements of § 14 DPA. If the level of data security is not to be lowered by the implementation of a Big Data application, such an application would have to provide at least the level of security that was provided by the most secure of the IT systems previously in use.[18] The previous maximum level of security therefore becomes the new minimum in a Big Data application.

Moreover, it has to be considered that, by operating a Big Data application, all data is collected in a single system, thus, "all eggs are put in a single basket." This results in an increase of risk because, previously, multiple systems would have had to be compromised in order to access all data, whereas now compromising a single system is sufficient. To mitigate this increase of risk, the implementation of additional security measures is necessary.

Furthermore, Big Data permits additional methods of analyzing data, *i.e.,* new possibilities to deduce new personal data from the existing data. This, too, constitutes an increase of risk that can be countered only by the implementation of new security measures.

Finally, Big Data typically results in new information flows,[19] *e.g.,* when data from the supply chain management (SCM) system and data from the customer relationship management (CRM) system are linked and processed for the purpose of human resources planning.[20]

   ISSN 1473-3579

This creates a new information flow from the SCM and CRM areas to human resources managers. Such new information flows not only create new risks in themselves but also raise the question whether the information security principle of "least privilege" can, at all, be implemented in a Big Data application. This principle provides that every program and every user of the system should operate using the least amount of privileges necessary to complete the job.[21] If a Big Data application is used to establish connections between data from different business areas (or areas of public administration), an unlimited access to all data pools is necessary. However, such an all-encompassing right of access to all data is not compatible with the principle of least privilege.

The principle of least privilege is also related to the requirement imposed by § 14(2)(5) DPA to define the access rights to data and programs. In this manner, logical access control, which is also one of the foundations of any security system,[22] may be very difficult to implement in a Big Data application. In particular, if the Big Data application contains unstructured, constantly changing data, it is virtually impossible to assign access rights manually. Any automated access control, *i.e.,* a Big Data-based security system that defines the access rights for individual data sets in a Big Data application, is, in principle, possible, but at this time hardly feasible from a technical perspective.

As regards the application of § 14 DPA to Big Data applications, it can be concluded that, in summary, Big Data creates numerous new risks and makes it nearly impossible to implement time-proven principles of information security. In order to comply with the requirements of § 14 DPA and to establish an adequate level of security commensurate with the heightened risks from Big Data applications, compensating security measures have to be implemented.

Legal Framework for Automated Individual Decisions

Big Data applications are sometimes also used to automate individual decisions, such as granting an overdraft on a debit account in accordance with § 23 Consumer Credit Act[23] or establishing the amount of bonuses granted to individual employees.

Since the results of a complex data analysis often have an "apparently objective and incontrovertible character to which a human decision-maker may attach too much weight,"[24] automated individual decisions carry an extraordinary risk and are therefore specifically addressed in Article 15 of the EU Data Protection Directive (Data Protection Directive) and § 49 DPA.

Pursuant to § 49(1) DPA, unless a statutory exception applies, nobody shall be subjected to a decision that 1) is fully automated, 2) is made on the basis of an evaluation of certain of the data subject's personal aspects, and 3) produces legal effects concerning the data subject or adversely affects him or her in a significant manner.

For a decision to be fully automated, the Big Data application not only has to provide a proposal for a decision but also has to predetermine that decision in a manner that 1) it is not formally made by a person and 2) no person is responsible for the substance of the decision.[25]

A "personal aspect" as referred to in the statute requires that the aspect has a certain complexity and is suitable as an object of evaluation. This follows from the examples provided by the statute: performance at work, creditworthiness, reliability, and conduct.[26] What is decisive is therefore not which categories of data are processed but rather whether the processing is performed for the purpose of evaluating a complex personal aspect of the data subject.[27]

The third element is that the decision produces legal effects for the data subject or adversely affects him or her in a significant manner. A legal effect can be produced not only by a decision made by a court or public authority but also by notices and declarations under civil law, such as the declaration to grant a loan or a contract termination notice.[28] Whether the legal effect is positive or negative for the data subject is, in principle, not relevant.[29]

However, a decision that "adversely affects [the data subject] in a significant manner" requires that the decision is valid *vis-à-vis* the data subject and has adverse consequences for him or her.[30] These requirements are fulfilled, for example, in the case of a rejected loan or job application,[31] but not in the case of a decision to send certain personalized ads to the data subject on the basis of results provided by a Big Data application,[32] or, in the case of a decision based on price differentiation,[33] to offer a reduced or increased price to the data subject in an online store.[34]

If all three above-described elements of § 49(1) DPA are present, a Big Data-based automated individual decision is prohibited unless any of the statutory exceptions discussed below applies:

Section 49(2) DPA provides three exceptions that permit automated individual decisions: 1) if the decision is expressly authorized by law (§ 49(2)(1) DPA); 2) if the decision is taken in the course of entering into or performance of a contract, provided the data subject's request for entering into or the performance of the contract has been satisfied (§ 49(2)(2) DPA); or 3) if the data subject's legitimate interests are safeguarded by appropriate means (§ 49(2)(3) DPA).

In two ways, these provisions are in contradiction to the Data Protection Directive. First, pursuant to Article 15(2)(b) Data Protection Directive, an authorization by law is sufficient only if it lays down measures to safeguard the data subject's legitimate interests.[35] Interpreting § 49(2)(1) DPA in accordance with the Data Protection Directive, this requirement has to be read into § 49(2)(1) DPA.[36]

Second, pursuant to Article 15(2)(a) Data Protection Directive but contrary to § 49(2)(3) DPA, the implementation of suitable measures to safeguard the data subject's legitimate interests is not an independent exception. The safeguarding of the data subject's interests is, pursuant to Article 15(2)(a) Data Protection Directive, rel-

evant only insofar as an automated individual decision that is taken in the course of the entering into or performance of a contract is permissible not only if the data subject's request for the entering into or the performance of the contract has been satisfied, but also, as an alternative, if the data subject's legitimate interests are safeguarded.

Interpreting § 49(2) DPA in conformance with the Data Protection Directive, an automated individual decision that is, in principle, prohibited by § 49(1) DPA is therefore permissible only by way of exception if 1) it is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests or 2) it is taken in the course of the entering into or performance of a contract with the data subject[37] and either a) the data subject's request for the entering into or the performance of the contract has been satisfied or b) there are suitable measures to safeguard the data subject's legitimate interests.[38]

The first exception (§ 49(2)(1) DPA) has no practical relevance for the private sector because there is no Austrian statute that would authorize automated individual decisions.

In connection with the second exception (§ 49(2)(2) in conjunction with § 49(2)(3) DPA), the question arises as to what is the meaning of the expression "taken in the course of the entering into or performance of a contract."

"[I]n the course of the entering into [. . .] a contract" has to be interpreted as also covering contract negotiations, irrespective of whether a contract is ultimately entered into. This follows from the fact that this exception is fulfilled not only if the data subject's request for the entering into the contract is satisfied (§ 49(2)(2) DPA) but also if the data subject's interests are safeguarded (§ 49(2)(3) DPA). "[I]n the course of the [. . .] performance of a contract" does not require that the decision was necessary for the performance. Rather, it should be considered sufficient that the automated individual decision has a clear connection to the performance. Thus, assuming all other requirements are fulfilled, a notice of contract termination is also covered by this exception.

If an automated decision made in connection with the contract satisfies the data subject's request for the entering into or performance of the contract, the requirements for the exception are fulfilled on this basis alone (§ 49(2)(2) DPA). For example, a Big Data-automated decision to grant a loan is permissible for this reason.[39]

On the other hand, if an automated decision is made that denies the data subject's request or an automated decision is taken that has no connection with a request by the data subject (*e.g.*, an automated contract termination), safeguarding the data subject's legitimate interests becomes paramount. In this regard, § 49(2)(3) DPA — in accordance with Article 15(2)(a) Data Protection Directive — identifies arrangements that allow the data subject to assert his or her point of view as an example of a suitable measure to safeguard the data subject's legitimate interests.

It is the generally held view that such arrangements would have to give the data subject the opportunity to assert his or her view before the automated decision is taken about the individual subject.[40] However, in our opinion, this view is not correct, because if such an opportunity is given before the decision is taken, the decision would not constitute a fully automated decision to which § 49 DPA would apply.[41]

To qualify for the exception provided for by § 49(2)(3) DPA, it is therefore sufficient to grant the opportunity to assert one's view *after* the automated decision about the individual has been taken if, upon receipt of the data subject's view, the final decision is suspended until it can be reviewed in a non-automated manner. This follows not only from the systematic considerations discussed above but also from the European Commission's comments to its amended proposal for the Data Protection Directive, dated 1992, where it was observed that the suspension of the final decision is sufficient.[42]

In contrast, the legislative materials of the DPA state that, for the private sector, the factual possibility alone to assert one's view would be sufficient because the data subject could, in any case, lodge his or her claims in civil court.[43] However, such an assertion of one's view which directly eliminates neither any legal effects nor significant adverse effects of the individual decision is not in compliance with the requirements established by the Data Protection Directive.[44]

In summary, to rely on the exception provided by § 49(2)(2) in conjunction with § 49(2)(3) DPA in connection with the entering into or performance of a contract is — if the data subject's request for the entering into or the performance of the contract is not satisfied — permissible only if 1) the data subject is informed of the automatic decision about the individual made by the Big Data application before that decision is implemented in reality and 2) the decision is suspended and subjected to a manual review where the data subject's point of view is received.

If an automated individual decision is permissible under the criteria described above, § 49(3) DPA mandates that, upon request, the data subject shall be "informed in an intelligible form of the logical procedure of the automated decision" within eight weeks.

In this regard, the legislative materials state that this disclosure obligation exists only insofar as it would not disproportionately interfere with third party rights, which would be the case if copyrights or trade secrets were put at risk.[45] Pursuant to Recital 41 of the Data Protection Directive, these considerations "must not, however, result in the data subject being refused all information." Therefore, a weighing of interests has to be performed regarding the extent of the disclosure.[46]

In traditional expert systems, the system developers manually assign certain significance values to different decision criteria which then produce the result of the decision. With such a system, the system operators are, in principle, required to disclose the relevant criteria as well as the respective significance of the decision criteria.[47] In a Big Data application, however, it is easily pos-

   ISSN 1473-3579

sible that the application itself dynamically defines the relevant criteria and their respective significance through an automatic analysis of the correlations between different data sets.

This meta-process for determining the relevant criteria and their respective significance is often treated as a trade secret by software manufactures. Therefore, the software manufactures' customers (the controllers) may not be able to disclose this meta-process. Depending on the specifics of the Big Data application, the implementation may allow the controller to obtain only the specific data that led to the decision but not the dynamically determined decision criteria or their respective significance.[48] In such a case, the logical procedure of the automated decision cannot be disclosed even to a limited extent; indeed, it cannot be disclosed at all. Thus, if the disclosure obligation pursuant to § 49(3) DPA cannot be complied with by the controller in any way, the use of a "Big Data Black Box" is, in effect, prohibited.

Limits Imposed by Fundamental Rights on the Use of Big Data in the Search for the Proverbial 'Needle in a Haystack'

At first glance, it appears effective to use Big Data applications also for the solution to problems where the proverbial needle is to be found in a haystack, *i.e.,* to identify a small number of individuals within a very large group of people. Possible areas of application in the private sector are the group-wide analysis of business e-mail correspondence and telephone traffic data in order to identify an employee among all group employees worldwide who committed industrial espionage or, in the public sector, the automatic identification of terrorists in the entire population by analyzing the totality of all traffic and location data, and contents of Internet and telephone communications of all residents. The activities of, in particular, the U.S. and the U.K. intelligence services which were publicly revealed in recent months[49] make it appear likely that such analyses are, indeed, performed in practice.

Such far-reaching processing of personal data of such large groups of data subjects raises numerous fundamental rights concerns in connection with § 1 DPA, Article 8 of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms,[50] and, as regards the implementation of EU law, Article 8 of the Charter of Fundamental Rights of the European Union.[51] Some of these concerns were debated extensively in connection with the EU Data Retention Directive (2006/24/EC).[52]

The following discussion is limited to one particular aspect of the use of Big Data for the search for the needle in the haystack: the low quality of the suspicion or incriminating circumstances created by such Big Data analyses.

If, for the sake of example, we assume that there are 100 terrorists within the EU's population of approximately 500 million people, and we further assume that a Big Data system existed and was being employed that, through the analysis of the entirety of all EU telephone and Internet communications, was capable of identifying terrorists with an accuracy of 99 percent — meaning correctly identify 99 of the 100 terrorists — one might conclude that this would be effective in producing actionable results, *i.e.,* that the people identified by the system as terrorists are, indeed, likely to be terrorists.

This incorrect assumption is based on the so-called base rate fallacy, which refers to the phenomenon that, when estimating probabilities, people tend to ignore the relative proportion of the target set to the full set (*i.e.,* the base rate).[53] In the above example, the Big Data analysis would identify 5,000,099 individuals as terrorists, where the probability of any particular such individual indeed being a terrorist would be only 0.0000198, *i.e.,* approximately 0.002 percent. This is because the system would have not only a hit ratio of 99 percent (and, thus, correctly identify 99 of the 100 terrorists as terrorists) but also an error rate of 1 percent, which results in the incorrect identification of 1 percent of the entire population, *i.e.,* 5 million, as terrorists.[54]

Even if it were possible to reduce the false positive rate from 1 percent to 0.01 percent — which appears highly unlikely in light of the difficulty to define a "profile of a terrorist" without falling into prejudiced stereotypes — 50,000 individuals would still be incorrectly identified and, thus, a total of 50,099 would be suspected as terrorists, where the probability of any such individual suspect indeed being a terrorist would be 0.00198, *i.e.,* approximately 0.2 percent.

However, such a low probability and therefore low level of suspicion does not, when taking into account the principle of proportionality, justify any further investigative measures against any one of the "suspects."[55] Thus, in such a case, the processing results obtained through Big Data are in effect worthless if the boundaries of fundamental rights are to be respected.

Thus, due to the low effectiveness, the public interest in conducting Big Data analyses for searching for a needle in a haystack is very low. Such blanket interference with fundamental rights is therefore disproportionate in light of the legally protected interests of the vast group of individuals concerned.

In conclusion, the use of Big Data applications to search for the proverbial needle in a haystack is largely impermissible.

Summary

Big Data brings about a change not only in the quantity of the data processed but also in the quality of the processing itself.

However, the Austrian DPA imposes significant limits on the use of Big Data. The very principles of data protection, specifically purpose specification and purpose limitation, often prohibit the transfer of existing data sets into a Big Data application. Furthermore, Big Data brings with it new risks, making the implementation of additional security measures necessary in order to comply with the requirements of § 14 DPA. When using Big Data applications, it also has to be considered that fully

automated individual decisions may be taken only within the tight limits of § 49 DPA and, even if permissible, require at least a partial disclosure of the decision logic, which is why the use of a "Big Data Black Box" is prohibited in this area. Lastly, the use of Big Data to find the proverbial needle in a haystack is often prohibited under the principle of proportionality.

NOTES

[1] *See* U.S. National Institute of Standards and Technology Big Data Public Working Group (NBD-PWG), Big Data Definitions, v1, NBD-WG: M0003 (2013), *available at* http://bigdatawg.nist.gov/_uploadfiles/M0003_v1_4301148665.docx.

[2] *See* Achim Born, *Raffinierte Daten — Aus Informationshalden wertvolle Erkenntnisse filtern [Refined Data — Gaining Valuable Insights from Information Dumps]*, iX, May 2013, at 86, 88 *et seq.* (F.R.G.).

[3] *See* Bitkom, *Big Data im Praxiseinsatz — Szenarien, Beispiele, Effekte [Big Data in Praxis — Scenarios, Examples, Effects]* 34 (2012), *available at* http://www.bitkom.org/de/publikationen/38337_73446.aspx (F.R.G.).

[4] Bundesgesetzblatt [BGBl] I No. 165/1999, as amended by BGBl I No. 83/2013. An official non-binding English translation is available at http://www.dsb.gv.at/DocView.axd?CobId=41936.

[5] *See* Rainer Knyrim, *Datenschutzrecht [Data Protection Law]* 77 (2nd ed. 2012) (Austria) (describing this challenge in connection with older phenomena such as data warehousing and data mining).

[6] The Data Retention Directive (2006/24/EC) serves as a prominent example: Irrespective of the plain language of its Article 1(1), it does not limit the processing purposes to the investigation, detection and prosecution of serious crime. Case C461/10, *Bonnier Audio AB v. Perfect Commc'n Sweden AB*, 2012 E.C.R. 00000,§ 43-45 = 2012 Medien und Recht International 29 (Austria); *see also* Lukas Feiler, *The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection*, 1 Eur. J. of L. & Tech. 3 (2010), *available at* http://ejlt.org//article/view/29/75, at n. 77.

[7] Since only a compatibility of the purposes is needed, it is a "weakened" principle of purpose limitation; *see* Ulrich Dammann & Spiros Simitis, *EG-Datenschutzrichtlinie [EC Data Protection Directive]* Article 8 cmt. 8 (1997) (F.R.G.).

[8] *See* Rainer Knyrim, *Datenschutzrecht [Data Protection Law]* 79 (2nd ed. 2012) (Austria) (stating that, for "marketing for own purposes," too, the compatibility with the original processing purpose is to be examined); *but see also* Alfred Duschanek & Claudia Rosenmayr-Klemenz, *Datenschutzgesetz 2000 [Data Protection Act 2000]* § 6 recital 3.2 (2000) (Austria).

[9] Nationalrat [NR] [National Council] Gesetzgebungsperiode [GP] 20 Beilage [Blg] No. 1613, at 52 (Austria).

[10] In practice, it is often a significant challenge to achieve true anonymization because the identity of the data subjects may still be inferred. *See* Austrian Data Protection Comm'n, case no. K213.180/0021-DSK/2013, May 22, 2013 (deciding over the transfer of supposedly anonymous statistics of groups of diseases by the Tyrolean public health insurance company to interested corporations).

[11] Nationalrat [NR] [National Council] Gesetzgebungsperiode [GP] 20 Beilage [Blg] No. 1613, at 51 (Austria).

[12] *Id.* at 52. This constitutes an "appropriate safeguard" within the meaning of Article 6(1)(b) Data Protection Directive. A "functional separation" that excludes the possibility that the obtained data are used for measures or decisions *vis-à-vis* individual data subjects is, however, not sufficient. As regards the concept of functional separation, *see* Article 29 Working Party, Opinion 03/2013 on purpose limitation 30, 46 (2013).

[13] As regards the statutory structure, *see also* Michael Suda, *Datenverwendung für wissenschaftliche Forschung und Statistik [Data Processing for Scientific Research and Statistics]*, in *Handbuch Datenschutzrecht [Handbook Data Protection Law]* 293, 302 (Lukas Bauer & Sebastian Reimer eds., 2009) (Austria); Dietmar Jahnel, *Handbuch Datenschutzrecht [Handbook Data Protection Law]* recital 8/11 (2010) (Austria).

[14] If a public grant has been obtained from an Austrian territorial authority or from the European Commission, the Austrian Data Protection Authority typically assumes that a public interest exists. Data Protection Comm'n, case no. K202.010/002-DSK/2001, April 24, 2001 = Walter Dohr *et al.,* DSG § 46 decision 2 (2nd ed. 2011) (Austria); Data Protection Comm'n, case no. K202.033/0003-DSK/2004, May 4, 2004. *See* Michael Suda, *Datenverwendung für wissenschaftliche Forschung und Statistik [Data Processing for Scientific Research and Statistics],* in *Handbuch Datenschutzrecht [Handbook Data Protection Law]* 293, 307 (Lukas Bauer & Sebastian Reimer eds., 2009) (Austria).

[15] A "transmission" is defined by § 4(12) DPA as "the transfer of data to recipients other than the data subject, the controller or a processor [. . .] as well as the use of data for another application purpose of the controller." *See* Dietmar Jahnel, *Handbuch Datenschutzrecht [Handbook Data Protection Law]* recitals 3/124 *et seq.*, 4/103 (2010) (Austria); *see, e.g.,* Oberster Gerichtshof [OGH] [Supreme Court], Feb. 25, 1992, 4 Ob 114/91 (Austria).

[16] *See* Ulrich Dammann & Spiros Simitis, *EG-Datenschutzrichtlinie [EC Data Protection Directive]* Article 17 cmt. 6 (1997) (F.R.G.) (stating that, ultimately, it was decisive how high the risks of an interference with the data subjects' rights and freedoms are).

[17] Whether a risk assessment should be performed on the basis of quantitative criteria (*e.g.,* potential damage of 100,000 euros; probability of damage of 0.03) or qualitative criteria (*e.g.,* "high" damages, "low" probability), has been the subject of debate for a long time. *See* Int'l Org. for Standardization [ISO] & Int'l Electrotechnical Comm'n [IEC], *Information technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary, ISO/IEC 27000:2009* § 2.34 (2009) and ISO & IEC, *Risk management — Risk assessment techniques, ISO/IEC 31010:2009* § 5.3.1 (2009) (respectively leaving this question unanswered). Quantitative approaches are clearly preferable because only these approaches can be verified. *See* extensively Lukas Feiler, *Information Security Law in the EU and the U.S.* 132 *et seq.* (2011) (providing further references).

[18] *See* Nat'l Inst. of Standards & Tech. [NIST], *Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards Publication 199*, at 4 (2004), *available at* http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf (also adopting this approach).

[19] *See* Christian Koot *et al.*, *Customer Lifetime Value mit Big Data — Neue Möglichkeiten zum systematischen Controlling von Kundenbeziehungen [Customer Lifetime Value with Big Data — New Possibilities for the Systematic Controlling of Customer Relationships]*, 2013 CFO aktuell 13, 13 (Austria).

[20] *See* Bernd Müller, *Der ungehobene Schatz [The Treasure to be Salvaged]*, Tech. Rev., March 2013, *available at* http://www.heise.de/tr/artikel/Der-ungehobene-Schatz-1808254.html (describing the planning of human resource requirements in a drug store chain).

[21] Jerome H. Saltzer & Michael D. Schroeder, *The Protection of Information in Computer Systems,* 63 Proceedings of the IEEE 1278, 1282 (1975).

[22] *See NIST, An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12*, at 195 *et seq.* (1995), *available at* http://csrc.nist.gov/publications/nistpubs/800-12/.

[23] *See* Kurier, *Job weg, Überziehungsrahmen weg [Job Lost, Overdraft Lost]*, http://kurier.at/wirtschaft/unternehmen/ams-und-bawag-job-weg-ueberziehungsrahmen-weg/20.504.372 (last accessed Nov. 5, 2013); Die Presse, *Bawag streicht AMS-Mitarbeitern Überziehungsrahmen [Bawag Removes Overdraft Right for Employees of Employment Agency]*, http://diepresse.com/home/meingeld/1434731/ (last accessed Nov. 5, 2013).

[24] *See* Amended Proposal of the European Commission, at 26, COM (92) 422 final (Oct. 15, 1992).

[25] Ulrich Dammann & Spiros Simitis, *EG-Datenschutzrichtlinie [EC Data Protection Directive]* Article 15 cmt. 3 (1997) (F.R.G.); Dietmar Jahnel, *Handbuch Datenschutzrecht [Handbook Data Protection Law]* recital 8/69 (2010) (Austria). *See* Walter Dohr *et al.,* DSG § 49 cmt. 5 (2nd ed. 2011) (Austria) (stating that is was necessary that the result of the processing was implemented as a decision without any modification).

[26] *See* Ulrich Dammann & Spiros Simitis, *EG-Datenschutzrichtlinie [EC Data Protection Directive]* Article 15 cmt. 4 (1997) (F.R.G.); Dietmar Jahnel, *Handbuch Datenschutzrecht [Handbook Data Protection Law]* recital 8/70 (2010) (Austria).

[27] *See* Dietmar Jahnel, *Handbuch Datenschutzrecht [Handbook Data Protection Law]* recital 8/70 (2010) (Austria); *but see* Ulrich Dammann & Spiros Simitis, *EG-Datenschutzrichtlinie [EC Data Protection Directive]* Article 15 cmt. 4 (1997) (F.R.G.) (arguing that the analysis of logs of input errors was, in any case, not covered).

   ISSN 1473-3579

[28] *See* Dietmar Jahnel, *Handbuch Datenschutzrecht [Handbook Data Protection Law]* recital 8/71 (2010) (Austria).

[29] Walter Dohr *et al.,* DSG § 49 cmt. 3 (2nd ed. 2011) (Austria).

[30] *See* Amended Proposal of the European Commission, at 26, COM (92) 422 final (Oct. 15, 1992).

[31] Ulrich Dammann & Spiros Simitis, *EG-Datenschutzrichtlinie [EC Data Protection Directive]* Article 15 cmt. 5 (1997) (F.R.G.).

[32] *Id.* (with reference to Amended Proposal of the European Commission, at 26, COM (92) 422 final (Oct. 15, 1992)).

[33] Regarding the practice of price differentiation (also "price discrimination") as a significant motivating factor for the collection of personal data, *see* Andrew Odlyzko, *Privacy, Economics, and Price Discrimination on the Internet*, in *Economics of Information Security* 187, 203 (L. Jean Camp & Stephen Lewis eds. (2004); Lukas Feiler, *Information Security Law in the EU and the U.S.* 36 *et seq.* (2011).

[34] Under Austrian civil law, such an "offer" constitutes only an *invitatio ad offerendum* and, thus, no decision that would have any legal effect; the decision also does not adversely affect the data subject in a significant manner because he or she would be free to purchase the goods from a competitor.

[35] *See* Ulrich Dammann & Spiros Simitis, *EG-Datenschutzrichtlinie [EC Data Protection Directive]* Article 15 cmt. 11 (1997) (F.R.G.).

[36] Dietmar Jahnel, *Handbuch Datenschutzrecht [Handbook Data Protection Law]* recital 8/71 (2010) (Austria); Alfred Duschanek & Claudia Rosenmayr-Klemenz, *Datenschutzgesetz 2000 [Data Protection Act 2000]* § 49 cmt. 2 (2000) (Austria).

[37] *See* Ulrich Dammann & Spiros Simitis, *EG-Datenschutzrichtlinie [EC Data Protection Directive]* Article 15 cmt. 10 (1997) (F.R.G.) (clarifying that only contracts concluded with the data subject are covered).

[38] *See also* Dietmar Jahnel, *Handbuch Datenschutzrecht [Handbook Data Protection Law]* recital 8/76 (2010) (Austria).

[39] *See* Walter Dohr *et al.,* DSG § 49 decision 10 (2nd ed. 2011) (Austria). *See also* Amended Proposal of the European Commission, at 27, COM (92) 422 final (Oct. 15, 1992).

[40] *See* Dietmar Jahnel, *Handbuch Datenschutzrecht [Handbook Data Protection Law]* recital 8/75 (2010) (Austria); Eugen Ehmann & Marcus Helfrich, *EG-Datenschutzrichtlinie [EC Data Protection Directive]* Article 15 cmt. 26 (1999) (F.R.G.); *see also* Ulrich Dammann & Spiros Simitis, *EG-Datenschutzrichtlinie [EC Data Protection Directive]* Article 15 cmt. 10 (1997) (F.R.G.) (stating that the controller should take the data subject's view into account when taking the decision).

[41] *See* Dietmar Jahnel, *Handbuch Datenschutzrecht [Handbook Data Protection Law]* recital 8/75 (2010) (Austria).

[42] Amended Proposal of the European Commission, at 27, COM (92) 422 final (Oct. 15, 1992).

[43] Nationalrat [NR] [National Council] Gesetzgebungsperiode [GP] 20 Beilage [Blg] No. 1613, at 53 (Austria).

[44] *See also* Dietmar Jahnel, *Handbuch Datenschutzrecht [Handbook Data Protection Law]* recital 8/75 (2010) (Austria) (with reference to Heinz Drobesch & Walter Grosinger, *Das neue österreichische Datenschutzgesetz [The New Austrian Data Protection Act]* § 15(2) cmt. 2 (2000) (Austria)).

[45] Nationalrat [NR] [National Council] Gesetzgebungsperiode [GP] 20 Beilage [Blg] No. 1613, at 53 (Austria).

[46] Austrian Data Protection Comm'n, case no. K121.313/0016-DSK/2007, Dec. 12, 2007.

[47] *Id.*

[48] *See* Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 Stanford L. Rev. Online 41 (2013) (referring to this as the transparency paradox).

[49] *See* Glenn Greenwald & Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, The Guardian, June 7, 2013, *available at* http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; Ewen MacAskill *et al., GCHQ taps fibre-optic cables for secret access to world's communications*, The Guardian, June 21, 2013, *available at* http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa; Glenn Greenwald, *XKeyscore: NSA tool collects 'nearly everything a user does on the internet,'* The Guardian, July 31, 2013, *available at* http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

[50] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 11, 1950, Council of Europe CETS No. 005, 213 U.N.T.S. 222.

[51] Charter of Fundamental Rights of the European Union, 2007 O.J. (C 303) 1.

[52] *See, e.g.,* Manuel Boka & Lukas Feiler, *Die Vorratsdatenspeicherung von Verkehrs- und Standortdaten [The Retention of Traffic and Location Data]*, in *Auf dem Weg zum Überwachungsstaat [On the Way to the Surveillance State]* 126, 152 *et seq.* (Wolfgang Zankl ed., 2009) (Austria); Birgit Kolb, *Vorratsdatenspeicherung [Data Retention]* 111 *et seq.* (2011) (Austria).

[53] *See* Amos Tversky & Daniel Kahneman, *Evidential Impact of Base Rates*, in *Judgment Under Uncertainty: Heuristics and Biases* 153 (Daniel Kahneman *et al.* eds., 1985); Douglas W. Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It* 101 (2009); Richards J. Heuer, *Psychology of Intelligence Analysis* 157 (2013).

[54] *See* Bruce Schneier, *Why Data Mining Won't Stop Terror*, Wired, March 9, 2006, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2006/03/70357?currentPage=all, *reprinted in Bruce Schneier, Schneier on Security* 9, 11 (2008).

[55] Any investigatory measures pursuant to the Austrian Criminal Procedure Statute require that there is a suspicion, *i.e.,* factual grounds justifying the assumption of a probability that certain facts are true; a mere speculation is not sufficient (*see* Ernst Markel, *Wiener Kommentar zur Strafprozessordnung [Viennese Commentary to the Criminal Procedure Code]* § 1 recital 26 (Helmut Fuchs & Eckart Ratz eds., 2014); Oberster Gerichtshof [OGH] [Supreme Court], holding no. RS0107304 (Austria)). Measures taken pursuant to the Austrian Security Police Act, too, are subject to the principle of proportionality; it has to be taken into account in particular whether the measure is directed against an innocent bystander. Sicherheitspolizeigesetz [SPG] [Security Police Act] Bundesgesetzblatt [BGBl] No. 566/1991, as amended, § 29(2)(2) (Austria).

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. Prof. Dr. Siegfried Fina, Ph.D., is an Associate Professor of European Union Law and Technology Law at the University of Vienna School of Law, a Visiting Professor at Stanford Law School and Co-Director of the Stanford-Vienna Transatlantic Technology Law Forum. He may be contacted at siegfried.fina@univie.ac.at.