Data Protection & Privacy 2020

Contributing editors
Aaron P Simpson and Lisa J Sotto

LEXOLOGY
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development managers
Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

First published 2012
Eighth edition
ISBN 978-1-83862-146-9

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Data Protection & Privacy

2020

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the eighth edition of *Data Protection and Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Hungary, Iceland, Indonesia and Malaysia.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
July 2019

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2019
For further information please contact editorial@gettingthedealthrough.com

Contents

Introduction 5
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

EU overview 9
Aaron P Simpson, Claire François and James Henderson
Hunton Andrews Kurth LLP

The Privacy Shield 12
Aaron P Simpson and Maeve Olney
Hunton Andrews Kurth LLP

Australia 16
Alex Hutchens, Jeremy Perier and Meena Muthuraman
McCullough Robertson

Austria 24
Rainer Knyrim
Knyrim Trieb Attorneys at Law

Belgium 32
David Dumont and Laura Léonard
Hunton Andrews Kurth LLP

Brazil 43
Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher and Thiago Luís Sombra
Mattos Filho

Chile 50
Carlos Araya, Claudio Magliona and Nicolás Yuraszeck
Magliona Abogados

China 56
Vincent Zhang and John Bolin
Jincheng Tongda & Neal

Colombia 66
María Claudia Martínez Beltrán and Daniela Huertas Vergara
DLA Piper Martínez Beltrán Abogados

France 73
Benjamin May and Farah Bencheliha
Aramis

Germany 83
Peter Huppertz
Hoffmann Liebs Partnerschaft von Rechtsanwälten mbB

Greece 90
Vasiliki Christou
Vasiliki Christou

Hungary 97
Endre Várady and Eszter Kata Tamás
VJT & Partners Law Firm

Iceland 104
Áslaug Björgvinsdóttir and Steinlaug Högnadóttir
LOGOS legal services

India 112
Stephen Mathias and Naqeeb Ahmed Kazia
Kochhar & Co

Indonesia 119
Abadi Abi Tisnadisastra, Prihandana Suko Prasetyo Adi and Filza Adwani
AKSET Law

Italy 126
Rocco Panetta and Federico Sartore
Panetta & Associati

Japan 136
Akemi Suzuki and Tomohiro Sekiguchi
Nagashima Ohno & Tsunematsu

Korea 144
Young-Hee Jo, Seungmin Jasmine Jung and Kwangbok Kim
LAB Partners

Lithuania 153
Laimonas Marcinkevičius
Juridicon Law Firm

Malaysia 159
Jillian Chia and Natalie Lim
Skrine

Malta 166
Ian Gauci and Michele Tufigno
Gatt Tufigno Gauci Advocates

Mexico 174
Abraham Díaz Arceo and Gustavo A Alcocer
OLIVARES

Netherlands **182**
Inge de Laat and Margie Breugem
Rutgers Posch Visée Endedijk NV

Portugal **188**
Helena Tapp Barroso and Tiago Félix da Costa
Morais Leitão, Galvão Teles, Soares da Silva & Associados

Russia **196**
Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva, Vasilisa Strizh and Brian Zimbler
Morgan, Lewis & Bockius LLP

Serbia **204**
Bogdan Ivanišević and Milica Basta
BDK Advokati

Singapore **212**
Lim Chong Kin
Drew & Napier LLC

Sweden **229**
Henrik Nilsson
Wesslau Söderqvist Advokatbyrå

Switzerland **236**
Lukas Morscher and Nadja Flühler
Lenz & Staehelin

Taiwan **245**
Yulan Kuo, Jane Wang, Brian, Hsiang-Yang Hsieh and Ruby, Ming-Chuang Wang
Formosa Transnational Attorneys at Law

Turkey **252**
Esin Çamlıbel, Beste Yıldızili and Naz Esen
TURUNÇ

United Kingdom **259**
Aaron P Simpson, James Henderson and Jonathan Wright
Hunton Andrews Kurth LLP

United States **268**
Lisa J Sotto and Aaron P Simpson
Hunton Andrews Kurth LLP

Austria

Rainer Knyrim
Knyrim Trieb Attorneys at Law

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The legislative framework for the protection of personally identifiable information (PII) in Austria mainly consists of the EU General Data Protection Regulation (GDPR) and the Data Protection Act (ADPA), which implements the mandatory opening clauses and provisions of the GDPR. In addition, the ADPA enshrines the fundamental right to data protection at the constitutional level. Furthermore, privacy-related provisions can be found, for example, in the Telecommunications Act regarding electronic advertising and the processing of personal communication data of users by telecommunication service providers; in the Act on Banking regarding banking secrecy; and in the Collective Labour Relations Act regarding data applications for purposes of personnel administration and evaluation. In the field of healthcare, the Health Telematics Act 2012 (along with the Health Telematics Regulation and the Federal Electronic Health Record Regulation 2013) states that technical data security measurements must be implemented for the transmission of health data among health service providers and contains provisions for the implementation and operation of the Federal Electronic Health Record. The Research Organisation Act regulates data processing for research purposes by scientific institutions.

Chapter 3 of the ADPA implements the Directive (EU) 2016/680 and regulates the processing of PII for purposes of the security police, including the protection of public security by the police, the protection of military facilities by the armed forces, the resolution and prosecution of criminal offences, the enforcement of sentences and the enforcement of precautionary measures involving the deprivation of liberty.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Data Protection Authority (DPA) will safeguard data protection in accordance with the provisions of the GDPR and the Federal Data Protection Act. The DPA will exercise its powers also in relation to the highest governing bodies or officers referred to in article 19 of the Federal Constitutional Law and in relation to the President of the National Council, the President of the Court of Auditors, the President of the Supreme Administrative Court and the Chairman of the Ombudsman Board in the area of the administrative matters to which they are entitled.

The DPA is established as a national supervisory authority pursuant to article 51 of the GDPR. The DPA acts as an authority supervising staff and as a human resource department. During his or her term of office, the head must not exercise any function that:

- could cast doubt on the independent exercise of his or her office or impartiality;
- prevents him or her from performing their professional duties; or
- puts essential official interests at risk.

The head is required to report functions that he or she exercises alongside his or her office as the head of the DPA to the Federal Chancellor without delay. The Federal Chancellor can request information from the head of the DPA on matters to be dealt with by the Authority. The head of the DPA has to meet this request only insofar as it does not impair the complete independence of the supervisory authority as described in article 52 of the GDPR.

Every data subject has the right to lodge a complaint with the DPA if he or she considers that the processing of his or her PII infringes the GDPR or section 1 of the ADPA.

The DPA will be responsible for imposing fines on natural and legal persons within the limits of its powers. Pursuant to section 11 of the ADPA, the DPA will apply the catalogue of article 83, paragraphs 2 to 6 of the GDPR in such a way that proportionality is maintained. In accordance with article 58 of the GDPR, the DPA will make use of its remedial powers, in particular by issuing warnings, especially in the event of initial infringements.

The ADPA empowers the DPA with further powers in addition to the investigative powers under article 58 of the GDPR. The DPA can request from the controller or the processor of the examined processing all necessary clarifications and inspect data-processing activities and relevant documents. The controller or processor shall render the necessary assistance. Supervisory activities are to be exercised in a way that least interferes with the rights of the controller or processor and third parties.

For the purposes of the inspection, the DPA will have the right, after having informed the owner of the premises and the controller or processor, to enter rooms where data-processing operations are carried out, put data-processing equipment into operation, carry out the processing operations to be examined and make copies of the storage media to the extent strictly necessary to exercise its supervisory powers.

In the case of a data-processing operation causing serious immediate danger to the interests of confidentiality of the data subject that deserves protection (imminent danger), the DPA may prohibit the continuation of the data-processing operation by an administrative decision pursuant to section 57, paragraph 1 of the General Administrative Procedure Act 1991. The continuation may also be prohibited only partially if this seems technically possible, meaningful with regard to the purpose of the data-processing operation and sufficient to eliminate the danger. At the request of a data subject, the DPA can also order, by an administrative decision pursuant to section 57, paragraph 1 of

the General Administrative Procedure Act, the restriction of processing pursuant to article 18 of the GDPR if the controller does not comply with an obligation to that effect within the period specified. If prohibition is not complied with immediately, the DPA will proceed pursuant to article 83, paragraph 5 of the GDPR.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches??

The rules governing cooperation between the lead supervisory authority and the other supervisory authorities concerned are laid down in article 60 of the GDPR. Article 61 of the GDPR provides for provisions on mutual assistance between the supervisory authorities. Pursuant to article 62 of the GDPR, the supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other member states are involved. In order to contribute to the consistent application of the GDPR, article 63 of the GDPR establishes a consistency mechanism according to which the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in section 2 of the GDPR.

Breaches of data protection

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Beside the penalty provisions under the GDPR, breaches of data protection regulations can lead to criminal or administrative penalties. The third chapter of the second main part of the ADPA provides specifying regulations regarding the implementation of remedies, liability and penalties. The implementation of administrative fines provides, to a certain extent, a possibility to impose fines primarily on legal persons.

The DPA shall be able to impose a fine on a legal person if one of its company organs or managers as decision maker or with a controlling position is subject to negligence or a breach of supervision. According to the concept of the Austrian administrative penal provisions, such fines would be imposed on the managing or executive board unless a responsible representative is appointed. The DPA shall refrain from imposing a fine on a responsible party pursuant to section 9 of the Administrative Penal Act 1991, if an administrative fine has already been imposed on the legal person for the same infringement.

No fines may be imposed on public authorities, public entities or public bodies, such as bodies established in particular under public or private law, which act on a statutory basis.

According to section 63 of the ADPA, whoever, with the intention of unlawfully enriching him or herself or a third party, or with the intention of damaging another person's claim guaranteed according to section 1, paragraph 1 of the ADPA, deliberately uses PII that has been entrusted to or has become accessible to him or her solely because of his or her professional occupation, or that he or she has acquired illegally, for him or herself or makes such data available to another person or publishes such data despite the data subject's interest in confidentiality, shall be punished by a court with imprisonment of up to one year unless the offence is subject to a more severe punishment pursuant to another provision.

Other provisions may be found in the Austrian Criminal Law, which contains rules for punishments in case of violations concerning data (eg, intentionally altering or deleting data).

Unless the offence meets the elements of article 83 of the GDPR or is subject to a more severe punishment according to other administrative penal provisions, an administrative offence punishable by a fine of up to €50,000 is committed by anyone who:

- intentionally and illegally gains access to data processing or maintains an obviously illegal access;
- intentionally transmits PII in violation of the rules on confidentiality and, in particular, intentionally uses data entrusted to him or her pursuant to the provisions granting the use of PII for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or of address data to inform or interview data subjects for other purposes;
- intentionally acquires PII in case of emergency under false pretences violating section 10 of the ADPA;
- processes images contrary to the provisions of Chapter 1, Part 3 of the ADPA; or
- refuses inspection pursuant to section 22, paragraph 2 of the ADPA.

Attempts shall be punishable. The penalty for the forfeiture of data storage media and programs as well as image transmission and recording devices may be imposed if these items are connected with an administrative offence.

The DPA shall be responsible for imposing fines on natural and legal persons within the limits of its powers. Pursuant to section 11 of the ADPA, the DPA will apply the catalogue of article 83, paragraphs 2 to 6 of the GDPR in such a way that proportionality is maintained. In accordance with article 58 of the GDPR, the DPA will make use of its remedial powers, in particular by issuing warnings, especially in the event of initial infringements.

SCOPE

Exempt sectors and institutions

5 Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

As a consequence of the constitutional status of the right for the protection of PII, the data protection law is applicable in all sectors. No type of organisation is exempted. Both public authorities and private organisations have to obey the rules imposed by data protection law. Pursuant to section 30, paragraph 5 of the ADPA, no fines may be imposed on authorities, public law corporate bodies or public entities – in particular entities established under public or private law, that act on a statutory basis.

Communications, marketing and surveillance laws

6 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Since each of these activities regularly leads to the electronic use of PII, the provisions of the GDPR and ADPA are generally applicable in these matters. Areas such as telecommunication or electronic marketing are regulated in the Telecommunications Act and the E-Commerce Act. The Criminal Law includes specific rules for punishments, for example, in the case of intentionally breaching the secrecy of telecommunication or abusively intercepting transferred data. The right to contradict the transmission of personally addressed advertisement material is defined in section 151, paragraph 11 of the Trade Regulation Act. Monitoring employees and appraising their performance is governed by the Collective Labour Relations Act, which, to the extent of the respective provisions, also forms part of Austrian data protection law. The ADPA regulates the permissibility of recording images and provides for special data security and labelling measures.

Other laws

7 | Identify any further laws or regulations that provide specific data protection rules for related areas.

A specific act exists for the transmission of health data among health service providers and for the Austrian Electronic Health Record, but with respect to the core regulations of data protection, this act refers to the GDPR. The same is true for regulations on credit information: credit information databases are mentioned in a few acts referring to data protection, which have incorporated general provisions to be applied to various areas connected to the processing of PII. The E Government Act provides regulations for a Federal Identity Management to enable authorities to identify people uniquely in governmental proceedings. The Act also regards aspects of data protection by defining an identity management system that prevents the possibility of merging PII across multiple authorities. If smart meters are used for the supply of electricity or gas, the applicable acts contain provisions for the protection of PII and grant customers the right to have their data accessed or transmitted via the internet (Electricity Industry and Organisation Act 2010, Gas Industry Act 2011). The Research Organisation Act establishes specific data protection regulations for scientific or historical research purposes or statistical purposes. Pursuant to the Collective Labour Relations Act, the implementation of control measures and technical systems for the control of employees, provided that these measures affect human dignity, require the consent of works councils in order to be legally valid.

PII formats

8 | What forms of PII are covered by the law?

In general, all activities regarding (partly) automatically processed PII are covered by the ADPA.

Extraterritoriality

9 | Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The GDPR applies to the processing of PII in the context of activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of PII of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or
- the monitoring of their behaviour as far as their behaviour takes place within the EU.

The ADPA applies to the use of PII in Austria, and outside Austria insofar as the data is used in other member states of the EU for the purposes of the main establishment or a branch establishment of the data controller in Austria. Apart from this general rule, however, the law of the state in which the data controller has its domicile applies where a data controller in the private sector whose seat is in another EU member state uses PII in Austria for purposes that cannot be attributed to any of the data controller's establishments in Austria. Furthermore, the ADPA shall not be applied insofar as the data is only transmitted through Austrian territory.

Covered uses of PII

10 | Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

The GDPR gives broad cover to the processing of PII; any type of processing such as collecting, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction is covered by its provisions.

The controller shall be responsible for, and be able to demonstrate the compliance with, the provisions and principles of the GDPR relating to the processing of PII. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject (article 28, paragraph 1 of the GDPR). Processing by a processor shall be governed by a contract or other legal act under EU or member state law that is binding on the processor with regard to the controller and sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of PII and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate the requirements laid down in article 28, paragraph 3 of the GDPR. Both the controller and the processor shall designate a data protection officer under certain conditions, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk and must keep a record of processing activities, whereas the content of the record of the processor must meet less stringent requirements.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 | Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Statutory provisions regarding the data subject's consent and legitimate purpose for processing and transmission of PII have been harmonised with the GDPR as set in Chapter 2 'Principles' of the GDPR.

In the case of an offer of information society services directly to a child, consent to the processing of PII of a child pursuant to article 6, paragraph 1(a) of the GDPR shall be lawful where the child is at least 14 years old (section 4, paragraph 4 of the ADPA).

Legitimate processing – types of PII

12 | Does the law impose more stringent rules for specific types of PII?

Pursuant to article 9, paragraph 1 of the GDPR, processing of special categories of PII (information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) shall be prohibited, unless a condition laid down in article 9, paragraph 2 of the GDPR is met.

The Health Telematics Act 2012 provides for special legal provisions for the electronic transfer of personal health data and genetic data.

Further, the ADPA contains reworded provisions for special data processing activities that are adapted to meet the preconditions of

the GDPR. The Austrian legislator reworded new provisions on 'image processing' that cover every observation of events. This leads to an extended scope (eg, photographs shall also be covered).

Processing PII on acts or omissions punishable by courts or administrative authorities, in particular concerning suspected criminal offences, as well as data on criminal convictions and precautionary measures involving the deprivation of liberty, is permitted if the requirements of the GDPR are met and if:

- an explicit legal authorisation or obligation to process such data exists; or
- the legitimacy of the processing of such data is otherwise based on statutory duties of diligence, or processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party pursuant to article 6, paragraph 1(f) of the GDPR, and the manner in which the data is processed safeguards the interests of the data subject according to the GDPR and the ADPA.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Pursuant to the provisions of the GDPR, controllers are required to provide information to data subjects whose PII is processed. If PII is collected directly from the data subject, the controller must provide information laid down in article 13 of the GDPR. If PII has not been obtained directly from the data subject, the controller has to provide, in addition to the information listed in article 13 of the GDPR, the categories of PII concerned from which source the PII originates and, if applicable, whether it came from publicly accessible sources (article 14 of the GDPR).

Exemption from notification

14 When is notice not required?

In addition to the exceptions pursuant to article 13, paragraph 4 and article 14, paragraph 5 of the GDPR, the Second Data Protection Amendment Act 2018 regulates exceptions from the obligation to provide information within the framework of the laws concerning healthcare professionals.

Control of use

15 Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The ADPA follows the provisions of the GDPR in this question. Section 4, paragraph 2 of the ADPA provides for a restriction of the right of rectification and the right to erasure. If PII processed by automated means cannot be rectified or erased immediately because it can be rectified or erased only at certain times for economic or technical reasons, processing of the PII concerned shall be restricted until that time, with the effect as stipulated in article 18, paragraph 2 of the GDPR.

Data accuracy

16 Does the law impose standards in relation to the quality, currency and accuracy of PII?

The GDPR applies directly and there are no stricter rules for principles relating to processing of PII set down in the ADPA. Therefore, PII must be accurate and kept up to date. Inaccurate or outdated data shall be deleted or amended, and data controllers are required to take 'every reasonable step' to comply with the principles set forth in the GDPR.

Amount and duration of data holding

17 Does the law restrict the amount of PII that may be held or the length of time it may be held?

Requirements regarding the amount and duration of data holding in the GDPR apply directly; there are no stricter rules or specifications for data storage durations set down in the ADPA. Specific storage periods can be found in the respective national material laws.

Finality principle

18 Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The GDPR applies directly and there are no stricter rules for principles relating to the processing of PII set down in the ADPA.

Use for new purposes

19 If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The ADPA does not require any other obligations regarding the processing of PII for purposes other than those for which the PII was initially collected than those set out in the GDPR.

Pursuant to section 7 of the ADPA, PII may be further used for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes under one of the following conditions:

- the PII is publicly accessible;
- the PII was initially collected lawfully by the controller for other research projects or other purposes;
- the PII is pseudonymised personal data for the controller, and the controller cannot establish the identity of the data subject by legal means;
- the PII is used for these purposes to a legal provision;
- the data subject has given his or her consent; or
- the DPA has given its approval.

Even in cases where the processing of PII for scientific research purposes or statistical purposes is permitted in a form that allows the identification of data subjects, the data shall be encoded without delay so that the data subjects are no longer identifiable if specific phrases of scientific or statistical work can be performed with pseudonymised data. Unless otherwise expressly provided for by law, data in a form that allows the identification of data subjects shall be rendered unidentifiable as soon as it is no longer necessary for scientific or statistical work to keep them identifiable.

The Research Organisation Act also specifies more detailed provisions for the processing of PII for research purposes by scientific institutions.

SECURITY

Security obligations

20 What security obligations are imposed on PII owners and service providers that process PII on their behalf?

The ADPA does not require any other or stricter obligations for the security of processing than those set out in the GDPR. Additionally, there are further provision for image processing (CCTV) regarding specific data security measures and labelling. Beside the duty of the controller

using image processing to disclose it appropriately, it has to be ensured that the access and manipulation of records by unauthorised persons are excluded. Any use of image processing has to be documented; this does not apply to real-time observation. Some of the material laws provide for specific data protection security obligations (eg, Research Organisation Act, Health Telematics Act 2012).

Notification of data breach

21 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Regarding this question, articles 33 and 34 of the GDPR apply directly without distinctions.

INTERNAL CONTROLS

Data protection officer

22 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The designation of a data protection officer (DPO) is mandatory under the conditions of article 37 of the GDPR.

The obligations of the DPO are laid down in section 5 of the ADPA. Without prejudice to other obligations of confidentiality, DPOs and persons working for the DPO shall be bound by confidentiality when fulfilling their duties. This shall apply in particular in relation to the identity of data subjects who applied to the DPO, and to circumstances that allow identification of these persons, unless the data subject has expressly granted a release from confidentiality. The DPO and persons working for the DPO may exclusively use information made available to fulfil their duties and shall be bound by confidentiality even after the end of their activities.

Section 5 of the ADPA provides for rules on the right of the DPO and persons working for the DPO to refuse to give evidence. Within the scope of the DPO's right to refuse to give evidence, his or her files and other documents are subject to a ban on seizure and confiscation.

Public-sector DPOs are not bound by any instructions when exercising their duties. The highest governing bodies or officers have the right to obtain information on matters to be dealt with from a public-sector DPO. The DPO shall only comply with this to the extent that this does not contradict the independence of the DPO within the meaning of article 38, paragraph 3 of the GDPR. Public-sector DPOs shall regularly exchange information, in particular with regard to ensuring uniform data protection standards.

Considering the type and scope of data-processing activities and depending on the facilities of a federal ministry, one or several DPOs shall be appointed in the sphere of responsibilities of each federal ministry. These DPOs shall be employed by the relevant federal ministry or the relevant subordinate office or other entity.

Record keeping

23 | Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

The GDPR applies directly. In order to demonstrate compliance with the GDPR, the controller or processor should maintain records of processing activities under their responsibility. Each controller and processor shall be obliged to cooperate with the supervisory authority and make those records available to the authority upon request.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

The ADPA does not alter the provisions of the GDPR, but Austrian legislation has made use of the opening clause of article 35, paragraph 10 of the GDPR with regard to certain legal provisions of national material laws and has carried out a data protection impact assessment as part of a general impact assessment in the context of the adoption of that legal provision (eg, Research Organisation Act).

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

According to current law, there is no legal obligation to notify or register data-processing activities with the supervisory authority. The former Austrian Data Processing Register held by the DPA shall be maintained by the DPA until 31 December 2019 for archiving purposes. No entries or changes in content have been made in the Data Processing Register since 25 May 2018. Registrations in the Data Processing Register become invalid. Any person may inspect the Register. Inspection of the registration file including any authorisations contained therein shall be granted if the person applying for inspection can satisfactorily demonstrate that he or she is a data subject, and as far as no overriding interests in confidentiality on the part of the controller or another person are an obstacle to access.

Formalities

26 | What are the formalities for registration?

There is no option to file a notification with the Data Processing Register because the obligation to notify is no longer applicable. The Data Processing Register is accessible online as an archive until December 2019.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

The provision regarding penalties is no longer applicable.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

The administrative procedure to register data applications was eliminated on 25 May 2018.

Public access

29 | Is the register publicly available? How can it be accessed?

Until December 2019, access to the Online Data Processing Register and its database is available at https://dvr.dsb.gv.at; from then on the internet platform will be discontinued.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

For changes under the Data Protection Amendment Act 2018, see question 25.

Other transparency duties

31 | Are there any other public transparency duties?

The GDPR is applicable directly. With regard to the processing of images, section 13, paragraph 5 of the ADPA stipulates a special obligation of disclosure.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Regarding this question, the rules regarding data processors, joint controllers and third parties under the GDPR apply directly without distinctions.

Restrictions on disclosure

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

The provisions of the GDPR apply directly. Specific restrictions concerning the disclosure of PII can be found in particular national laws (eg, Research Organisation Act).

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

The provisions of the GDPR apply directly. Pursuant to the provisions of the GDPR, international data transfer outside of the EU is similar to the existing regime under the Data Protection Directive. Data can be transferred under a Commission Adequacy Decision (eg, EU–US Privacy Shield, Standard Contractual Clauses, Binding Corporate Rules or the explicit consent of the data subject).

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

The GDPR applies directly and there are no stricter rules set down in the ADPA.

Further transfer

36 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The GDPR applies directly and there are no stricter rules set down in the ADPA.

RIGHTS OF INDIVIDUALS

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

The right to access data is part of the rights of data subjects in connection with transparency. The GDPR stipulates which information has to be provided where PII is collected from the data subject. Pursuant to section 4, paragraph 5 of the ADPA, the right to access pursuant to article 15 of the GDPR does not apply to a controller acting on a statutory basis, without prejudice to other legal restrictions, if the provision of such access jeopardises the performance of a task assigned to the controller by law. Furthermore, the right to access pursuant to article 15 of the GDPR does generally not apply to a controller, without prejudice to other legal restrictions, if the disclosure of such information would endanger a business or trade secret of the controller or third parties (section 4, paragraph 6 of the ADPA).

Other rights

38 | Do individuals have other substantive rights?

Besides the right of access, data subjects have the right to request from the controller rectification or erasure of PII or restriction of processing concerning the data subject or to object to processing, as well as the right to data portability. Furthermore, data subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Compensation

39 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The GDPR allows data subjects to take action against data protection violations, in addition to any imposed administrative fines under the GDPR. The subject may address civil courts in order to receive compensation for any material or non-material damage suffered as a result of a GDPR infringement. Non-material damages can be compensated under Austrian civil law. The ADPA also provides a choice of the competent court in whose jurisdiction the place of the domicile of the data subject and the seat of the defendant is situated.

Enforcement

40 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Every data subject has the right to lodge a complaint with the DPA if the data subject is of the opinion that the processing of PII infringes the GDPR or the ADPA. The Federal Administrative Court shall decide through a panel of judges on complaints against administrative decisions of the DPA. Furthermore, each data subject can apply to the Federal Administrative Court if the DPA does not handle a complaint or does not inform the data subject within three months of the progress or outcome of the complaint lodged.

Under the ADPA, data subjects are entitled to mandate a non- profit-organisation body, organisation or association that has been properly constituted, has statutory objectives that are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their PII to lodge the complaint on his or her behalf and to exercise the rights referred to in sections 24 to 27 of the ADPA. On the other hand, the ADPA does not provide the opportunity to assign specialised organisations (data protection NGOs) to file claims for damages with the responsible civil court.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 | Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Section 9 of the ADPA implements the opening clause provided by article 85 of the GDPR. The processing of PII by media owners, editors, copy editors and employees of a media undertaking or media service

within the meaning of the Media Act, for journalistic purposes of the media undertaking or media service, the provisions of the ADPA and Chapters II, III, IV, V, VI, VII and IX of the GDPR shall not apply. When exercising its powers towards the persons named in the first sentence, the DPA must observe the protection of editorial confidentiality (section 31 of the Austrian Media Act).

If it is necessary to reconcile the right to protection of personal data with the freedom of expression and information, Chapters II (with the exception of article 5), III, IV (with the exception of articles 28, 29 and 32), V, VI, VII and IX do not apply to processing for purposes of academic, artistic or literary expression. Of the provisions of the ADPA, section 6 (confidentiality of data) shall be applied in such cases.

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

Data subjects may appeal against decisions of the DPA to the Federal Administrative Court and may further appeal against decisions of the Federal Administrative Court to the Supreme Administrative Court.

SPECIFIC DATA PROCESSING

Internet use

43 | Describe any rules on the use of 'cookies' or equivalent technology.

These issues have to be evaluated under general principles and according to the provisions of the GDPR and the Telecommunications Act respectively. As the EU ePrivacy Directive 2002/58/EC has been amended by Directive 2009/136/EC, new special regulations for the declaration of consent for the use of cookies on websites had to be translated to the Telecommunications Act.

Austria implemented the EU ePrivacy Directive in November 2011 and has simply translated article 5, paragraph 3 of the Directive into section 96, paragraph 3 of the Telecommunications Act.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

Both the Telecommunications Act and the e-Commerce Act contain provisions for commercial communications and sanctions for 'cold-calling' and unsolicited faxes and emails. Commercial calls and the transmission of commercial messages are only legitimate with the recipient's prior consent. Some exceptions exist for the transmission of emails. Violating these provisions could lead to a fine of up to €37,000 for each unlawful email or up to €58,000 for each cold call respectively.

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

The ADPA does not contain specific rules regarding the use of cloud computing services. Hence, the general provisions of the GDPR are applicable. As cloud service providers are often located outside the EEA, international data transfer needs special attention (see question 34).

According to the Health Telematics Act 2012, it has to be ensured that health data is saved in storage that is provided based on the needs of clients ('cloud computing') only if the health data has been encrypted using state-of-the-art technology (section 6, paragraph 1 No. 2 of the Health Telematics Act 2012).

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Network and Information Systems Security Act

In order to implement the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union Austria introduced the Network and Information Systems Security Act (NISG) in December 2018. It's main aim is to ensure a high level of security of network and information systems mainly by

- strengthening cooperation between member states to elaborate national NIS strategies;
- setting up national authorities and computer emergency teams (in Austria: cert.at, sector specific certs and GovCert); and
- requiring certain private and public operators of public interest to take appropriate safety measures and to report significant incidents.

The law is targeted at private and public operators of critical social and economic sectors (energy, transport, banking, financial market infrastructures, healthcare, drinking water delivery and supply, digital infrastructure) and providers of digital services (online marketplaces, online search engines, cloud computing services) with operating subsidiaries within the EU, which are reliant on network and information systems and where a security incident could cause a significant disruption in the provision of their services. It stipulates that respective operators and providers must implement certain safety standards and immediately report security incidents to the responsible computer emergency team to prevent further threats.

Act Against Unfair Competition (business secrets amendment)

To implement the Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure Austria amended the Act Against Unfair Competition (UWG) in January 2019. This led to a plus in legal certainty – not only for the protection of know-how per se, but also for owners of business secrets.

The amendment introduced a legal definition of 'business secret' to the Act Against Unfair Competition, encapsulating that it has to be secret, of commercial value and object to appropriate confidentiality measures (the latter depending on the type of secret, business field and company size).

Among other things, independent discovery or creation as well as 'reverse engineering' are permitted. On the other hand, acquisition is prohibited (among other things) if it is caused by unauthorised access or appropriation or if a contractual agreement or an non-disclosure agreement is violated in the process. Anyone who unlawfully acquires, uses or discloses business secrets may be sued for injunctive relief, removal and, in the event of culpability, for damages. Any profits of the infringer from the illegal acquisition, illegal use or illegal disclosure can be claimed by the holder of the trade secret as well as compensation for financial loss. Furthermore, the holder of the trade secret has a right to the publication of a judgment against the infringer, and the protection of the confidentiality of business secrets in the course of court proceedings has been increased.

Draft for Austrian Digital Tax Act 2020

In order to take account of the progressing digitalisation, a digital tax is to be introduced with effect from 1 January 2020. The draft for the Digital Tax Act 2020 is currently under revision. As in various other

EU member states, the Digital Tax Act 2020 is also intended to make a contribution to increasing tax equity. Certain services of the 'digital economy' related to Austria are to be taxed. The proposal is also based on the Digital Advertising Tax Proposal, which was not approved by all EU member states in March 2019. The previous advertising tax under the Advertising Tax Act 2000 only covered 'classic' advertising in print media, radio and television, on posters and other forms of toleration of the use of space and rooms for advertising purposes. The digital tax is now also intended to cover online advertising.

The Digital Tax Act 2020 also aims to achieve the easiest possible flat-rate taxation with automated procedures. To be able to react as flexibly as possible to new developments and experiences in the field of the 'digital economy', the Federal Minister of Finance is to be authorised to make appropriate adjustments by way of ordinance.

Draft for Austrian Act on Diligence and Responsibility on the Net

To facilitate the prosecution of legal claims in the event of illegal web-postings and to promote the respectful interaction of posters in online forums the draft for the Act on Diligence and Responsibility on the Net is currently under revision. The Act aims to oblige service providers who operate discussion forums or enabling the establishment of a forum to verify the identity of the posters; only after successful completion of the registration profile should the user be able to publish postings in this forum.

Users must create a registration profile and register, stating in each case their first name and surname; the obligations according to which the personal data are to be transmitted to courts or administrative authorities are determined by the draft as well. Service providers are held to appoint a responsible representative, in particular as a delivery agent.

KNYRIM.TRIEB
RECHTSANWÄLTE

Rainer Knyrim
kt@kt.at

Mariahilfer Straße 89A
1060 Vienna
Austria
Tel: +43 1 909 30 70
Fax: +43 1 909 36 39
www.kt.at

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

ISBN 978-1-83862-146-9