Data Protection & Privacy 2022

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 manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Tenth edition
ISBN 978-1-83862-644-0

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

Data Protection & Privacy

2022

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

Lexology Getting The Deal Through is delighted to publish the tenth edition of *Data Protection & 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 Jordan, Pakistan and Thailand.

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 2021

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2021
For further information please contact editorial@gettingthedealthrough.com

Contents

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

EU overview 11
Aaron P Simpson, David Dumont, James Henderson and Anna Pateraki
Hunton Andrews Kurth LLP

The Privacy Shield 14
Aaron P Simpson and Maeve Olney
Hunton Andrews Kurth LLP

Australia 20
Alex Hutchens, Jeremy Perier and Meena Muthuraman
McCullough Robertson

Austria 28
Rainer Knyrim
Knyrim Trieb Rechtsanwälte

Belgium 37
David Dumont and Laura Léonard
Hunton Andrews Kurth LLP

Brazil 49
Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher and Thiago Luís Sombra
Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados

Canada 57
Doug Tait and Kendall N Dyck
Thompson Dorfman Sweatman LLP

Chile 65
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya
Magliona Abogados

China 72
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo
Mayer Brown

France 82
Benjamin May and Marianne Long
Aramis Law Firm

Germany 96
Peter Huppertz
Hoffmann Liebs Fritsch & Partner

Hong Kong 104
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo
Mayer Brown

Hungary 113
Endre Várady and Eszter Kata Tamás
VJT & Partners Law Firm

India 121
Arjun Sinha, Mriganki Nagpal and Siddhartha Tandon
AP & Partners

Indonesia 128
Rusmaini Lenggogeni and Charvia Tjhai
SSEK Legal Consultants

Israel 136
Adi El Rom and Hilla Shribman
Amit Pollak Matalon & Co

Italy 145
Paolo Balboni, Luca Bolognini, Davide Baldini and Antonio Landi
ICT Legal Consulting

Japan 154
Akemi Suzuki and Takeshi Hayakawa
Nagashima Ohno & Tsunematsu

Jordan 164
Ma'in Nsair, Haya Al-Erqsousi and Mariana Abu-Dayah
Nsair & Partners - Lawyers

Malaysia 170
Jillian Chia Yan Ping and Natalie Lim
SKRINE

Malta 178
Paul Gonzi and Sarah Cannataci
Fenech & Fenech Advocates

Mexico 187
Abraham Díaz and Gustavo A Alcocer
OLIVARES

New Zealand 195
Derek Roth-Biester, Megan Pearce and Victoria Wilson
Anderson Lloyd

Pakistan 202
Saifullah Khan and Saeed Hasan Khan
S.U.Khan Associates Corporate & Legal Consultants

Portugal 209
Helena Tapp Barroso and Tiago Félix da Costa
Morais Leitão, Galvão Teles, Soares da Silva & Associados

Romania 218
Daniel Alexie, Cristina Crețu, Flavia Ștefura and Alina Popescu
MPR Partners

Russia 226
Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva and Alena Neskoromyuk
Morgan, Lewis & Bockius LLP

Serbia 235
Bogdan Ivanišević and Milica Basta
BDK Advokati

Singapore 242
Lim Chong Kin
Drew & Napier LLC

Sweden 257
Henrik Nilsson
Wesslau Söderqvist Advokatbyrå

Switzerland 265
Lukas Morscher and Leo Rusterholz
Lenz & Staehelin

Taiwan 276
Yulan Kuo, Jane Wang, Brian Hsiang-Yang Hsieh and Ruby Ming-Chuang Wang
Formosa Transnational Attorneys at Law

Thailand 284
John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Patchamon Purikasem
Formichella & Sritawat Attorneys at Law Co, Ltd

Turkey 291
Esin Çamlıbel, Beste Yıldızili Ergül, Naz Esen and Nazlı Bahar Bilhan
Turunç

United Kingdom 299
Aaron P Simpson, James Henderson and Jonathan Wright
Hunton Andrews Kurth LLP

United States 309
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Austria

Rainer Knyrim

Knyrim Trieb Rechtsanwälte

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 PII in Austria mainly consists of Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) and the Data Protection Act (DPA), which implements the mandatory opening clauses and provisions of the GDPR. Also, the DPA enshrines the fundamental right to data protection at the constitutional level. Further, privacy-related provisions can be found in:

- the Telecommunications Act regarding electronic advertising and the processing of personal communication data of users by telecommunication service providers;
- the Act on Banking regarding banking secrecy; and
- 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 DPA implements Directive (EU) 2016/680 (the Law Enforcement Directive) 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 (the Authority) will safeguard data protection under the provisions of the GDPR and the DPA. The Authority will exercise its powers also concerning the highest governing bodies or officers referred to in article 19 of the Federal Constitutional Law and concerning 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 Authority is established as a national supervisory authority under article 51 of the GDPR. The Authority 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 Authority to the Federal Chancellor without delay. The Federal Chancellor can request information from the head of the Authority on matters to be dealt with by the Authority. The head of the Authority 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 Authority if he or she considers that the processing of his or her PII infringes the GDPR or section 1 of the DPA.

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

The DPA empowers the Authority 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 Authority 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 Authority may prohibit the continuation of the data processing operation by an administrative decision under 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 regarding the purpose of the data processing operation and sufficient to eliminate the danger. At the request of a data subject, the Authority can also order, by an administrative decision under section 57, paragraph 1 of the General Administrative Procedure Act, the restriction of processing under 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 Authority will proceed under 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. Under 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. 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 European 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?

Besides 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 DPA 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 Authority shall be able to impose a fine on a legal person if one of its company organs or managers as a 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 Authority shall refrain from imposing a fine on a responsible party under 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 DPA, whoever, to unlawfully enrich him or herself or a third party, or intending to damage another person's claim guaranteed according to section 1, paragraph 1 of the DPA, 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 more severe punishment under another provision.

Other provisions may be found in the Austrian Criminal Law, which contains rules for punishments in the 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 obviously illegal access;
- intentionally transmits PII in violation of the rules on confidentiality and, in particular, intentionally uses data entrusted to him or her under 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 the case of emergency under false pretences violating section 10 of the DPA;
- processes images contrary to the provisions of Chapter 1, Part 3 of the DPA; or
- refuses inspection under section 22, paragraph 2 of the DPA.

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

The Authority shall be responsible for imposing fines on natural and legal persons within the limits of its powers. Under section 11 of the DPA, the Authority will apply the catalogue of article 83, paragraphs 2 to 6 of the GDPR in such a way that proportionality is maintained. Under article 58 of the GDPR, the Authority 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 personally identifiable information (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. Under section 30, paragraph 5 of the Data Protection Act (DPA), 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 DPA 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 DPA 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 the Austrian Electronic Health Record, but concerning 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 (the Electricity Industry and Organisation Act 2010 and the Gas Industry Act 2011). The Research Organisation Act establishes specific data protection regulations for scientific or historical research purposes or statistical purposes. Under 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, requires the consent of works councils 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 DPA.

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 European Union, regardless of whether the processing takes place in the European Union or not. The GDPR also applies to the processing of PII of data subjects who are in the European Union by a controller or processor not established in the European Union, 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 European Union; or
- the monitoring of their behaviour as far as their behaviour takes place within the European Union.

Section 3 of the DPA has been deleted, hence there is no specific regulation beyond that of the GDPR.

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 compliance with, the provisions and principles of the GDPR relating to the processing of PII. Where the 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 EU member state law that is binding on the processor regarding 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.

Two or more controllers who jointly determine the purposes and means of processing shall be joint controllers. They shall determine their respective responsibilities in an agreement in a transparent manner, in particular regarding the exercising of the rights of the data subject and their respective duties to provide the information referred to in articles 13 and 14, unless and in so far as the respective responsibilities of the controllers are determined by law. The agreement shall clearly state that there is a joint responsibility, how each controller participates in deciding on the purposes and means of joint processing and that controller fulfils which obligations determined by the GDPR. The agreement must disclose the relationships between the joint controllers, in particular the nature of the cooperation. These relationships can be of a legal nature but also reflect factual circumstances. The agreement should also state a contact point for data subjects.

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 Regulation (EU) 2016/679 (the General Data Protection Regulation) (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 under 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 Data Protection Act (DPA)).

Legitimate processing – types of PII

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

Under 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 to uniquely identify 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 DPA 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). The Federal Administrative Court assumes that the provisions on image processing of the DPA are in breach of EU law due to the lack of opening clauses in the GDPR and are therefore not applicable.

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 the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party under article 6, paragraph 1(f) of the GDPR, and how the data is processed safeguards the interests of the data subject according to the GDPR and the DPA.

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?

Under the provisions of Regulation (EU) 2016/679 (the General Data Protection Regulation) (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 under 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 Data Protection Act (DPA) follows the provisions of the GDPR in this question. Section 4, paragraph 2 of the DPA 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 the processing of PII set down in the DPA. 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 outlined 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 DPA, apart from a rule in article 4(2) of the DPA permitting the storage of data until the next periodic deletion date, if the data is deleted periodically due to technical or commercial circumstances. 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 DPA.

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 DPA generally does not permit the processing of PII for purposes other than those for which the PII was originally collected. However, there are exceptions:

Under section 7 of the DPA, 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 Data Protection Authority 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 Data Protection Act (DPA) does not require any other or stricter obligations for the security of processing than those set out in Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR). Additionally, there are further provisions for image processing (CCTV) regarding specific data security measures and labelling. Besides 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. The Federal Administrative Court assumes that the provisions on image processing of the DPA are in breach of EU law due to the lack of opening clauses in the GDPR and are therefore not applicable.

Some of the material laws provide for specific data protection security obligations (eg, the Research Organisation Act and the 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?

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 Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR).

The obligations of the DPO are laid down in section 5 of the Data Protection Act (DPA). 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 concerning 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 the information made available to fulfil their duties and shall be bound by confidentiality even after the end of their activities.

Section 5 of the DPA 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 regarding 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. 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 DPA 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 regarding 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, the 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 Data Protection Authority (the Authority) was maintained by the Authority until 31 December 2019 for archiving purposes and has been shut down. No entries or changes in content had been made in the Data Processing Register since 25 May 2018.

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 former Data Processing Register is not accessible online.

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?

Access to the Online Data Processing Register has been closed.

Effect of registration

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

An entry on the register that has been effective before 25 May 2018 may exclude the Controller from the duty to conduct a Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) data protection impact assessment (DPIA) due to the DPIA White List published by the Authority.

Other transparency duties

31 | Are there any other public transparency duties?

The GDPR is applicable directly. Regarding the processing of images, section 13, paragraph 5 of the Data Protection Act stipulates a special obligation of disclosure. The Federal Administrative Court assumes that the provisions on image processing of the DPA are in breach of EU law due to the lack of opening clauses in the GDPR and are therefore not applicable.

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 Regulation (EU) 2016/679 (the General Data Protection Regulation) (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, the Research Organisation Act).

Cross-border transfer

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

The provisions of the GDPR apply directly. Under the provisions of the GDPR, international data transfer outside of the European Union is similar to the existing regime under Directive 95/46/EC (the Data Protection Directive). Data can be transferred under a European Commission Adequacy Decision (eg, standard contractual clauses, binding corporate rules or the explicit consent of the data subject).

Due to the Court of Justice of the European Union decision in *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (case C-311/18), *Schrems II*, in cases where standard contractual clauses are put in place, the legal situation in the data recipient's country must be examined up front.

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 Data Protection Act (DPA).

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 DPA.

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. Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) stipulates that information has to be provided where PII is collected from the data subject. Under section 4, paragraph 5 of the Data Protection Act (DPA), the right to access under 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. Further, the right to access under 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 DPA).

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. Further, 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 act against data protection violations, in addition to any imposed administrative fines under the GDPR. The subject may address civil courts 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 DPA 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. The Supreme Court referred the following questions to the Court of Justice of the European Union in this regard:

- Does the award of damages under article 82 GDPR require, in addition to a breach of provisions of the GDPR, that the plaintiff has suffered damage or is the infringement as such sufficient?
- Are there other requirements under EU law for the assessment of damages in addition to the principles of effectiveness and adequacy?
- Is it compatible with EU law that a consequence of the infringement of rights, with at least some weight that goes beyond the annoyance caused by the infringement itself, is a prerequisite for the award of non-material damages?

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 Data Protection Authority (the Authority) if the data subject believes that the processing of PII infringes the GDPR or the DPA. The Federal Administrative Court shall decide through a panel of judges on complaints against administrative decisions of the Authority. Further, each data subject can apply to the Federal Administrative Court if the Authority 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 DPA, 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 regarding 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 DPA. On the other hand, the DPA does not provide the opportunity to assign specialised organisations (data protection non-governmental organisations) to file claims for damages with the responsible civil court.

Under section 29(2) of the DPA, the Regional Court of First Instance has jurisdiction over the claim for damages, irrespective of the amount in dispute, which also results in an absolute obligation to be represented by a lawyer. The appointment of a senate (one chairman and two members) to decide on the claim can be requested by both the claimant (in the claim) and the defendant (in the defence) from an amount in dispute exceeding €100,000 under section 7a(1) of the Austrian Jurisdictional Standards. In the case of disputes between employers and employees in connection with the employment relationship, for example, in the case of the processing of personal data of employees by the employer, the labour and social courts have jurisdiction under section 3 of the Labour and Social Courts Act (the ASGG) in connection with section 50(1)(1) of the ASGG. In cases of public liability (ie, claims for damages against the federal government, provinces, districts, municipalities, other public corporations and the social insurance institutions), the regional court also has jurisdiction under section 9 of the Public Liability Act.

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 Data Protection Act (DPA) implements the opening clause provided by article 85 of Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR). The processing of personally identifiable information (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 DPA and Chapters 2, 3, 4, 5, 6, 7 and 9 of the GDPR shall not apply. When exercising its powers towards the persons named in the first sentence, the Data Protection Authority 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 2 (except for article 5), 3, 4 (except for articles 28, 29 and 32), 5, 6, 7 and 9 do not apply to processing for purposes of academic, artistic or literary expression. Of the provisions of the DPA, 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 Data Protection Authority 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 Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) and the Telecommunications Act respectively. Since Directive 2002/58/EC (the ePrivacy Directive) was amended by Directive 2009/136/EC (the Citizen's Rights Directive), 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. Providers of an information society service are obliged to inform the user which personal data they will process, on what legal basis and for what purposes this will be done and for how long the data will be stored. The collection of this data is only permissible if the user has given his or her consent. This shall not prevent technical storage or access if this is strictly necessary for the provider of an information society service expressly requested by the user to be able to provide that service. The Telecommunications Act explicitly only refers to personal cookies. The regulation is therefore contrary to EU law as the regulation should also cover non-personal data.

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 Data Protection Act (DPA) 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 European Economic Area, international data transfer needs special attention.

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?

Investigations by the Data Protection Authority

In the first half of 2020, businesses in Austria were subject to in-depth investigations by the Data Protection Authority (the Authority).

One trend seen in these investigations is that the Authority received files from other data protection authorities of EU member states about complaints from data subjects based in those member states, where those authorities' investigations revealed the data processing activities were performed by, or responsibility for them rested with, an Austrian group of companies.

Another emerging trend is that the Authority is actively accusing the managers of companies – and even the managers and chief executives of parent or grandparent companies – for failures in General Data Protection Regulation compliance and privacy management.

Many proceedings with fines under article 83 of Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) concern the unlawful operation of image processing systems in and outside private buildings and vehicles (dashcams).

Also, the data protection authority imposed fines on police officers for accessing the police's electronic file system without being able to prove that they had any official reason to access the data.

Accreditation

The DPA stipulates that the accreditation of a certification body can solely be carried out by the data protection authority itself. To be accredited as a certification body, a comprehensive application is required, which, among other things, describes the independence, the expertise as well as the organisational structure under the requirements of the Certification Bodies Accreditation Regulation. To maintain public confidence, certification criteria shall be approved, a certification scheme with certification requirements shall be developed and a management system for continued, impartial and non-discriminatory task performance shall be operated. The certification body must carry out its activities independently, confidentially, impartially and in a documented manner.

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

Coronavirus

47 | What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programmes, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

Section 5c of the Austrian Epidemics Act (AEA) is the legal basis for the collection of contact data in restaurants. The contact data of guests was collected for transmission to the authorities upon request in the event of a covid-19 case. However, the data protection authority believed that there was no sufficient legal basis for this.

Since December 2020, there is an authorisation for regulations on the mandatory registration of contact data, for example, by the operators of restaurants, where it is 'absolutely necessary and proportionate' due to the pandemic. If an ordinance based on section 5c(1) of the AEA is issued, section 5c(1) of the AEA obliges not only the restaurant operators to collect data, but also the data subjects to provide their data.

Since May 2021, there has been a covid-19 restaurant opening regulation. Operators of restaurants may only allow customers to enter if they show evidence of low epidemiological risk. Such evidence includes:

- proof of a negative covid-19 antigen test result;
- medical confirmation of infection in the past six months;
- proof of vaccination with a centrally approved vaccine; or
- proof of neutralising antibodies.

Section 25a of the AEA

This provision creates a legal basis within the meaning of article 6(1)(e) in conjunction with (2) and (3) of the GDPR for the processing of personal data by public authorities. If it is stipulated that certain data must be disclosed upon entry from particular countries, this provision constitutes the legal basis for the digital or analogue transmission of these data to the district administrative authority of the place of residence or stay of the person entering the country.

Section 24(ff) of the Austrian Health Telematics Act

This provision creates a legal basis for the processing of health data according to article 9(2)(g)–(j) of the GDPR. To ensure the public interest, the federal minister responsible for healthcare must operate the eHealth

application Electronic Vaccination Certificate as the controller. An essential component of this application is a central vaccination register, which serves as the electronic documentation of all vaccinations carried out. Information on the vaccine, the administered vaccination, the individual citizens and the vaccinating or storing healthcare provider is stored. For statistical evaluations, especially for the determination of vaccination coverage rates, the personal data stored in the central vaccination register must be encrypted.

Labour law

Every employer has an obligation of care towards its employees, which includes the exclusion of health risks at the workplace. Therefore, the processing of health data can be based on article 9(2)(b) of the GDPR in conjunction with the relevant provisions. For the transfer of health data to the health authorities, article 9(2)(i) of the GDPR in conjunction with section 10(2) of the DPA provides a corresponding legal basis. Also, at the request of the district administrative authorities, there may also be an obligation on the part of the employer to provide information (about suspected cases and infections) under article 9, paragraph 2(i) of the GDPR in conjunction with section 5(3) of the Epidemic Act 1950.

Stopp Corona app

In Austria, it is also possible to register contacts via the Stopp Corona app, which records encounters with other app users using Bluetooth and the exchange of numerical codes. According to article 6(1)(a) of the GDPR, coronavirus tracking is based on the app's user consent.

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
Business & Human Rights
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
Drone Regulation
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
Healthcare M&A
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
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
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

an LBR business

ISBN 978-1-83862-644-0