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

Pakistan

Saifullah Khan and Saeed Hasan Khan

S.U.Khan Associates Corporate & Legal Consultants

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?

Pakistan is in the process of developing a dedicated law on personal data protection. The Ministry of Information Technology & Telecommunication has developed a draft of the law, the Personal Data Protection Bill 2020 (the draft Bill). The draft Bill has passed the consultation stage and will now be presented to the Federal Cabinet for approval before presenting the same to the legislature, the National Assembly and Senate, for promulgating the law. PII is called 'personal data' in the draft Bill to mean any information that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data controller, including any sensitive personal data, provided that anonymised, encrypted or pseudonymised data that is incapable of identifying an individual is not personal data. The answers to the following questions are based upon the draft Bill. The draft Bill largely follows the General Data Protection Regulation of the European Union.

Data protection authority

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

The federal government, under the draft Bill, is to establish an authority to be known as the Personal Data Protection Authority of Pakistan (the Authority). On promulgation of the law (the draft Bill becoming an Act), the federal government will establish the Authority. The Authority, under the draft Bill, shall be responsible to carry out the purposes of the draft Bill. The Authority shall be competent to decide complaints and pass any order. To decide complaints the Authority shall be deemed to be Civil Court and shall have the same powers as are vested in the Civil Court. The Authority shall be empowered to formulate a compliance framework concerning data audits. The Authority may require a data controller or a data processor to provide such information to the Authority as may reasonably be required for effective discharging of functions of the Authority.

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 draft Bill provides that the Authority may, subject to prior approval of the federal government, cooperate with any foreign authority or international organisation in the field of data protection, data security, data theft or unlawful data transfer. The cooperation is to be based on the terms and conditions of any programme or agreement for cooperation to which such foreign authority or international organisation is a party or pursuant to any other international agreement made after the commencement of the draft Bill.

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?

The draft Bill provides for the following penalties concerning contravention of the provisions of the draft Bill:

Offence	Fine/imprisonment
A data controller not ceasing the processing of personal data after withdrawal of consent by the data subject	A fine of up to 5 million Pakistani rupees or imprisonment for a term not exceeding three years or both
Anyone who processes or causes to be processed, disseminates or discloses personal data in violation of the draft Bill	A fine of up to 15 million Pakistani rupees and in the case of subsequent unlawful processing the fine may be raised to 25 million Pakistani rupees. In the case of sensitive data, the fine may be raised to 25 million Pakistani rupees
Failure to adopt the security measures that are necessary to ensure data security	A fine of up to 5 million Pakistani rupees
Failure to comply with the orders of the Authority	A fine of up to 2.5 million Pakistani rupees
Corporate liability on a legal person	A fine not exceeding 1% of its annual gross revenue in Pakistan or 30 million Pakistani rupees, whichever is greater

The Authority will be empowered to formulate a compliance framework concerning personal data breach and grievance redressal mechanism. Once this compliance framework is formulated then it will be clear as to how to deal with such breaches.

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?

The draft Bill applies to all sectors and types of organisations. However, it provides an exemption to specific processing from a few specified requirements, as follows:

- the prevention or detection of crime or for investigations;
- the apprehension or prosecution of offenders;
- the assessment or collection of tax or duty or any other imposition of a similar nature;
- preparing statistics or carrying out research (provided that resulting statistics or results of the research are not made available in a form that identifies the data subject);
- the connection with any order or judgment of a court;
- the discharging of regulatory functions (if the application whereof would be likely to prejudice the proper discharge of those functions); and
- journalistic, literary or artistic (subject to certain conditions).

The above-stated are exempted from the following requirements:

- the general requirements (of lawful purpose, purpose limitation, data minimisation and consent);
- notice to the data subject;
- non-disclosure; and
- adherence to the security standards prescribed by the Personal Data Protection Authority of Pakistan (the Authority).

Also, the processing concerning the physical or mental health of data subject is exempted from the applicability of security standards prescribed by the Authority if application whereof would be likely to cause serious harm to the physical or mental health of the data subject or any other individual.

Apart from the above, the federal government, on the recommendation of the Authority, may exempt any data controller or class of data controllers from the application of any provision of the draft Bill.

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.

The draft Bill does not cover interception of communication, electronic marketing or monitoring and surveillance of individuals.

The Investigation for Fair Trial Act 2013 provides for investigation for collection of evidence through modern techniques and devices to prevent and effectively deal with certain specified offences.

The Monitoring and Reconciliation of Telephony Traffic Regulations 2010 deals with controlling grey traffic. These Regulations are applicable for licences issued by the Pakistan Telecommunication Authority for:

- long-distance and international;
- infrastructure or landing station;
- local loop (fixed and wireless); and
- cellular mobile.

Other laws

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

- Banking:
  - the Payment Systems and Electronic Fund Transfers Act 2007;
  - the State Bank of Pakistan (SBP) Regulations for Payment Card Security; and
  - the SBP Regulations for Security of Internet Banking;
- telecommunication:
  - the Telcom Consumer Protection Regulations 2009;
  - the Regulations for Technical Implementation of Mobile Banking 2016; and
  - the Critical Telecom Data and Infrastructure Security Regulations 2020; or
- healthcare:
  - the Pakistan Medical and Dental Council Code of Ethics of Practice for Medical and Dental Practitioners.

PII formats

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

The draft Bill covers personal data in an all-inclusive way (any information that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data controller, including any sensitive personal data, provided that anonymised, encrypted or pseudonymised data that is incapable of identifying an individual is not personal data). The draft Bill covers all processing of personal data whether or not by automated means.

Extraterritoriality

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

The draft Bill has extraterritorial applicability. The draft Bill is applicable if any of the data subjects, the data controller or data processor is located in Pakistan. A data controller or data processor who is not registered or established in Pakistan is to nominate a representative in Pakistan for the purposes of the draft Bill.

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 draft Bill applies to the processing of personal data either by a data controller or by a data processor.

'Data controller' means a natural or legal person or the government, who either alone or jointly has the authority to decide on the collection, obtaining, usage or disclosure of personal data.

'Data processor' means a natural or legal person or the government who alone or in conjunction with others processes data on behalf of the data controller.

The draft Bill places significant obligations on the data controllers and there are lessor obligations on the data processors as compared to data controllers. The data processors, however, are responsible for ensuring compliance with security standards prescribed by the Authority. The Authority is empowered to formulate a compliance framework for data processors. A complaint can also be filed against both the data controllers and data processors.

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?

Section 5 of the draft Bill lays down the general requirements for personal data collection and processing. Personal data shall not be processed unless:

- the personal data is processed for a lawful purpose directly related to an activity of the data controller;
- the processing of the personal data is necessary for, or directly related to, that purpose; and
- the personal data is adequate but not excessive concerning that purpose.

A data controller, under the draft Bill, shall not process personal data unless the data subject has given his or her consent. Following are the exceptions to have consent:

- for the performance of a contract to which the data subject is a party;
- for taking steps at the request of the data subject to enter into a contract;
- for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by a contract;
- to protect the vital interests of the data subject;
- for the administration of justice pursuant to an order of the court of competent jurisdiction;
- for legitimate interests pursued by the data controller; or
- for the exercise of any functions conferred on any person by or under any law.

Legitimate processing – types of PII

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

To process sensitive personal data the draft Bill requires to have 'necessity' in addition to consent. The draft Bill provides that sensitive personal data can only be processed if the processing is necessary:

- to exercise or perform any right or obligation that is conferred or imposed by law on the data controller in connection with employment;
- to protect the vital interests of the data subject or another person, in a case where:
  - consent cannot be given by or on behalf of the data subject; or
  - the data controller cannot reasonably be expected to obtain the consent of the data subject;
- to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;
- for medical purposes and is undertaken by:
  - a healthcare professional; or
  - a person who in the circumstances owes a duty of confidentiality that is equivalent to that which would arise if that person were a healthcare professional;
- for, or in connection with, any legal proceedings;
- to obtain legal advice while ensuring its integrity and secrecy;
- to establish, exercise or defend legal rights;
- for the administration of justice pursuant to orders of a court of competent jurisdiction; or
- for the exercise of any functions conferred on any person by or under any written law.

Sensitive personal data can also be processed if the information contained in the data has been made public as a result of steps deliberately taken by the data subject.

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?

A data controller shall, by written notice, inform a data subject:

- that personal data of the data subject is being collected and a description of the personal data;
- on the legal basis for the processing of personal data;
- on the duration for which personal data is likely to be processed and retained thereafter;
- on the purpose for which the personal data is being collected or is to be collected and further processed;
- on the information of the source of the personal data (if available with the data controller);
- on the data subjects' right to request access and correction of personal data and how to contact the data controller concerning any inquiries or complaints;
- on the class of third parties to whom the data controller discloses or may disclose the personal data;
- on the choices and means the data controller offers to the data subject for limiting the processing of personal data;
- whether it is obligatory or voluntary for the data subject to supply personal data; and
- where it is obligatory to supply personal data, the consequences on the data subject for failure to do so.

Notice is required to be given:

- when the data subject is first asked by the data controller to provide his or her personal data;
- when the data controller first collects the personal data of data subject;
- before the data controller uses the data subject's personal data for a purpose other than the purpose for which it was collected;
- before the data controller discloses the personal data to a third party; and
- in the national and English languages, and the individual (data subject) be provided with a clear and readily accessible means to exercise his or her choice.

Exemption from notification

14 When is notice not required?

Notice is not required to be given in the case the personal data is processed for:

- the prevention or detection of crime or for investigations;
- the apprehension or prosecution of offenders;
- the assessment or collection of tax or duty or any other imposition of a similar nature;
- preparing statistics or carrying out research (provided that resulting statistics or results of the research are not made available in a form which identifies the data subject);
- the connection with any order or judgment of a court;
- the discharging of regulatory functions (if the application whereof would be likely to prejudice the proper discharge of those functions); and
- journalistic, literary or artistic (subject to certain conditions).

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?

Section 25 of the draft Bill confers a right on the data subjects to ask the data controller to cease the processing, or cease the processing for a specified purpose, or cease the processing in a specified manner. The data subject may also ask the data controller not to begin the processing, or not to begin the processing for a specified purpose or not to begin processing in a specified manner if the same is causing or is likely to cause substantial damage or substantial distress to him or a relevant person and that the damage or distress is or would be unwarranted.

Data accuracy

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

The draft Bill requires that a data controller is to take reasonable steps to ensure that personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose including any directly related purpose for which personal data was collected and further processed.

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?

The draft Bill requires that personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose. The data controller is required to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.

Finality principle

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

Section 5.2 of the draft Bill (while discussing the general requirements for collection and processing of personal data) requires that personal data shall not be processed unless the processing is necessary for, or is directly related to, a lawful purpose directly related to an activity of the data controller (purpose limitation principle).

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 purpose limitation principle is not applicable in the case of the following processing:

- the prevention or detection of crime or for investigations;
- the apprehension or prosecution of offenders;
- the assessment or collection of tax or duty or any other imposition of a similar nature;
- preparing statistics or carrying out research (provided that resulting statistics or results of the research are not made available in a form that identifies the data subject);
- the connection with any order or judgment of a court;
- the discharging of regulatory functions (if the application whereof would be likely to prejudice the proper discharge of those functions); and
- journalistic, literary or artistic (subject to certain conditions).

SECURITY

Security obligations

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

The draft Bill requires that a data controller or a data processor while processing the personal data, are to take practical steps to protect the personal data following the security standards prescribed by the Personal Data Protection Authority of Pakistan (the Authority). The Authority is to prescribe security standards to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

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?

In the event of a personal data breach the data controller is to:

- notify the Authority in respect of the breach;
- notify without any delay and not beyond 72 hours; and
- give reasons for the delay in the case the notification is made beyond 72 hours.

An exception to the above is where the breach is unlikely to result in a risk to the rights and freedoms of the data subject.

Information to be provided in the Personal Data Breach Notification includes:

- the description and nature of the personal data including (where possible) the categories and approximate number of concerned data subjects, and the categories and approximate number of concerned personal data records;
- the name and contact details of the data protection officer or another contact from where more information can be obtained;
- the likely consequences of the breach; and
- the measures adopted or proposed to be adopted by the data controller to address the breach.

There is no requirement to give breach notification to the data subject.

INTERNAL CONTROLS

Data protection officer

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

There is no expressed requirement in the draft Bill; however, while discussing the power of the Personal Data Protection Authority of Pakistan (the Authority), the draft Bill confers upon it the power to formulate responsibilities of the Data Protection Officer. Therefore, the Authority, when established, will devise the appointment requirements.

Record keeping

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

The draft Bill requires that a data controller is to keep and maintain a record of any application, notice, request or any other information relating to personal data that has been or is being processed. The

Authority is empowered to determine the manner and form in which the record is to be maintained.

New processing regulations

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

There is no expressed requirement in the draft Bill; however, while discussing the power of the Authority, the draft Bill confers upon it the power to formulate a compliance framework regarding data protection impact assessment. Therefore, the Authority, when established, will devise such a framework.

REGISTRATION AND NOTIFICATION

Registration

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

There is no expressed requirement in the draft Bill; however, while discussing the power of the Personal Data Protection Authority of Pakistan (the Authority), the draft Bill confers upon it the power to devise a registration mechanism for data controllers and data processors. Therefore, the Authority, when established, will devise the registration requirements.

Formalities

26 | What are the formalities for registration?

None.

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?

None.

Refusal of registration

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

None.

Public access

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

None.

Effect of registration

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

None.

Other transparency duties

31 | Are there any other public transparency duties?

There are no such duties under the draft Bill.

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?

In such cases, the data controller is to ensure that the data processor undertakes to adopt applicable technical and organisational security standards governing the processing of personal data as prescribed by the Personal Data Protection Authority of Pakistan (the Authority).

Restrictions on disclosure

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

The draft Bill requires that personal data without the consent of the data subject shall not be disclosed for any purpose other than the purpose for which the same was to be disclosed at the time of collection. The personal data shall not be disclosed to any party other than a third party already notified to the data subject.

Cross-border transfer

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

The draft Bill provides that if personal data is required to be transferred to any system located beyond the territories of Pakistan or any system that is not under the direct control of any of the governments in Pakistan, it must be ensured that the country where the data is being transferred offers personal data protection at least equivalent to the protections provided under the draft Bill. The personal data so transferred shall be processed under the draft Bill. Critical personal data shall only be processed in Pakistan. The federal government is vested with the power to exempt certain categories of personal data (except sensitive data) from these requirements on the grounds of necessity or strategic interests.

Notification of cross-border transfer

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

The Authority is empowered to devise a framework under which personal data may be transferred outside Pakistan. Once the Authority is established, the framework related to the transfer of personal data outside Pakistan will be devised.

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 Authority is empowered to devise a framework under which personal data may be transferred outside Pakistan. Once the Authority is established, the framework related to the transfer of personal data outside Pakistan will be devised.

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 draft Bill confers the right on the data subject to have access or a copy of his or her personal data held by the data controller. The data subject on payment of a prescribed fee makes a request in writing to the data controller. A data controller may refuse to comply with the request on the following grounds:

- the data controller is not supplied with such information as the data controller may reasonably require;
- the data controller cannot comply with the request without disclosing personal data relating to another individual who can be identified from that information;
- any other data controller controls the processing of personal data to which request relates in such a way as to prohibit the first-mentioned data controller from complying;
- providing access may constitute a violation of an order of a court;
- providing access may disclose confidential information relating to the business of the data controller; and
- access to personal data is regulated by another law.

Other rights

38 Do individuals have other substantive rights?

The draft Bill confers the following rights on the data subjects:

- the right to correct personal data;
- the right to withdrawal of consent;
- the right to prevent processing likely to cause damage or distress; and
- the right to erasure.

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 draft Bill does not provide for any damages or compensation to the data subjects.

Enforcement

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

Rights to the data subjects are enforced by the Personal Data Protection Authority of Pakistan (the Authority). Any decision or order of the Authority is appealable at a higher forum.

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.

The draft Bill applies to all sectors and types of organisations. However, it provides an exemption to specific processing from a few specified requirements, as follows:

- the prevention or detection of crime or for investigations;
- the apprehension or prosecution of offenders;
- the assessment or collection of tax or duty or any other imposition of a similar nature;
- preparing statistics or carrying out research (provided that resulting statistics or results of the research are not made available in a form that identifies the data subject);
- the connection with any order or judgment of a court;
- the discharging of regulatory functions (if the application whereof would be likely to prejudice the proper discharge of those functions); and
- journalistic, literary or artistic (subject to certain conditions).

The above-stated are exempted from the following requirements:

- the general requirements (of lawful purpose, purpose limitation, data minimisation and consent);
- notice to the data subject;
- non-disclosure; and
- adherence to the security standards prescribed by the Personal Data Protection Authority of Pakistan (the Authority).

Also, the processing concerning the physical or mental health of data subject is exempted from the applicability of security standards prescribed by the Authority if application whereof would be likely to cause serious harm to the physical or mental health of the data subject or any other individual.

Apart from the above, the federal government on the recommendation of the Authority may exempt any data controller or class of data controllers from the application of any provision of the draft Bill.

SUPERVISION

Judicial review

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

The orders of the Personal Data Protection Authority of Pakistan are appealable before the High Court or to any other tribunal established by the federal government for the purposes in the manner prescribed by the High Court.

SPECIFIC DATA PROCESSING

Internet use

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

No rules exist on the use of 'cookies'.

Electronic communications marketing

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

No rules exist concerning marketing by email, fax or telephone.

Cloud services

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

No rules exist concerning the use of cloud computing services.

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?

The Ministry of Information Technology & Telecommunication has recently issued a consultation draft of the National Cyber Security Policy 2021. One of the significant aspects of the policy is to develop the Cyber Security Act and develop rules and regulations for the national cybersecurity framework. It is expected that on finalisation of the subject policy, work on the drafting of the Cyber Security Act will begin.

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?

In 2020, the Supreme Court of Pakistan and several High Courts condoned the time limitation in filing appeals or petitions for a certain period owing to the coronavirus situation. The best practices, advisable to clients, include the use of technology to work during the lockdown and to follow all safety measures. As the use of technology has been increased significantly (eg, working from home), it is important to pay particular attention to data security while transferring or communicating business-sensitive information through electronic means.

S.U.Khan Associates
Corporate & Legal Consultants

Saifullah Khan
saifullah.khan@sukhan.com.pk

Saeed Hasan Khan
saeed.hasan@sukhan.com.pk

First Floor, 92-Razia Sharif Plaza
Fazal-ul-Haq Road
Blue Area
Islamabad (44000)
Pakistan
Tel +92 51 2344741 |
Fax +92 51 2344743
www.sukhan.com.pk

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