

International Comparative Legal Guides



Data Protection 2020

A practical cross-border insight into data protection law

Seventh Edition

Featuring contributions from:

Addison Bright Sloane
Anderson Mōri & Tomotsune
Chandler MHM Limited
Clyde & Co
DDPV Studio Legale
Deloitte Kosova Shpk
Deloitte Legal Shpk
D'LIGHT Law Group
DQ Advocates Limited
Drew & Napier LLC
Elzaburu S.L.P.
FABIAN PRIVACY LEGAL GmbH
Herbst Kinsky Rechtsanwälte GmbH
Homburger AG

Khaitan & Co LLP
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys-at-Law
Leśniewski Borkiewicz & Partners
LPS L@w
LYDIAN
Marval O'Farrell Mairal
Matheson
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
NEOVIAQ IP/ICT
Nyman Gibson Miralis
OLIVARES

Pellon de Lima Advogados
PPM Attorneys
Rothwell Figg
Semenov&Pevzner
SEOR Law Firm
SKW Schwarz Rechtsanwälte
SSEK Indonesian Legal Consultants
S. U. Khan Associates
Corporate & Legal Consultants
Synch Advokatpartnerselskab
Templars
White & Case LLP
White & Case, s.r.o., advokátní kancelář
Wikborg Rein Advokatfirma AS

Expert Chapters

- 1** **The Rapid Evolution of Data Protection Laws**
Dr. Detlev Gabel & Tim Hickman, White & Case LLP
- 6** **Privacy, Data Protection, and Cybersecurity: A State-Law Analysis**
Martin M. Zoltick & Jenny L. Colgate, Rothwell Figg
- 12** **Privacy By Design in Digital Health**
Daniela Fábíán Masoch, FABIAN PRIVACY LEGAL GmbH
- 17** **Initiatives to Boost Data Business in Japan**
Takashi Nakazaki, Anderson Mōri & Tomotsune

Q&A Chapters

- 24** **Albania**
Deloitte Legal Shpk: Ened Topi & Aida Kaloci
- 33** **Argentina**
Marval O'Farrell Mairal: Gustavo P. Giay & Diego Fernández
- 42** **Australia**
Nyman Gibson Miralis: Dennis Miralis & Phillip Gibson
- 54** **Austria**
Herbst Kinsky Rechtsanwälte GmbH:
Dr. Sonja Hebenstreit
- 65** **Belgium**
LYDIAN: Bastiaan Bruyndonckx & Olivia Santantonio
- 77** **Brazil**
Pellon de Lima Advogados: Rafael Pellon & Nathalia Santos
- 86** **China**
King & Wood Mallesons: Susan Ning & Han Wu
- 97** **Cyprus**
Koushos Korfiotis Papacharalambous LLC:
Loizos Papacharalambous & Anastasios Kareklas
- 109** **Czech Republic**
White & Case, s.r.o., advokátní kancelář: Ivo Janda & Anna Stárková
- 119** **Denmark**
Synch Advokatpartnerselskab: Christine Jans & Heidi Højmark Helveg
- 131** **France**
Clyde & Co: Benjamin Potier & Pierre Affagard
- 141** **Germany**
SKW Schwarz Rechtsanwälte: Nikolaus Bertermann
- 150** **Ghana**
Addison Bright Sloane: Victoria Bright & Justice Oteng
- 159** **India**
Khaitan & Co LLP: Harsh Walia & Supratim Chakraborty
- 169** **Indonesia**
SSEK Indonesian Legal Consultants:
Denny Rahmansyah & Raoul Aldy Muskitta
- 178** **Ireland**
Matheson: Anne-Marie Bohan & Chris Bollard
- 190** **Isle of Man**
DQ Advocates Limited: Kathryn Sharman & Sinead O'Connor
- 200** **Israel**
Naschitz, Brandes, Amir & Co., Advocates:
Dalit Ben-Israel & Efrat Artzi
- 211** **Italy**
DDPV Studio Legale: Luciano Vasques & Chiara Sciarra
- 223** **Japan**
Mori Hamada & Matsumoto: Hiromi Hayashi & Masaki Yukawa
- 234** **Korea**
D'LIGHT Law Group: Iris Hyejin Hwang & Hye In Lee
- 244** **Kosovo**
Deloitte Kosova Shpk: Ardian Rexha & Ened Topi
- 253** **Luxembourg**
NEOVIAQ IP/ICT: Raymond Bindels & Milan Dans
- 264** **Mexico**
OLIVARES: Abraham Díaz Arceo & Gustavo Alcocer
- 273** **Nigeria**
Templars: Emmanuel Gbahabo & Oghomwen Akpaibor
- 286** **Norway**
Wikborg Rein Advokatfirma AS: Gry Hvidsten & Emily M. Weitzenboeck
- 298** **Pakistan**
S. U. Khan Associates Corporate & Legal Consultants: Saifullah Khan & Saeed Hasan Khan
- 306** **Poland**
Leśniewski Borkiewicz & Partners:
Grzegorz Leśniewski, Mateusz Borkiewicz & Jacek Cieśliński
- 317** **Russia**
Semenov&Pevzner: Ekaterina Smirnova
- 326** **Senegal**
LPS L@w: Léon Patrice Sarr

Q&A Chapters Continued

335

Singapore

Drew & Napier LLC: Lim Chong Kin

349

South Africa

PPM Attorneys: Delphine Daversin & Melody Musoni

359

Spain

Elzaburu S.L.P.: Ruth Benito Martín & Alberto López Casalilla

370

Switzerland

Homburger AG: Dr. Gregor Bühler, Luca Dal Molin & Dr. Kirsten Schmidt

379

Taiwan

Lee and Li, Attorneys-at-Law: Ken-Ying Tseng & Sam Huang

389

Thailand

Chandler MHM Limited: Pranat Laohapairoj Mori Hamada & Matsumoto: Atsushi Okada

397

Turkey

SEOR Law Firm: Okan Or & Basak Feyzioglu

407

United Kingdom

White & Case LLP: Tim Hickman & Matthias Goetz

417

USA

White & Case LLP: Steven Chabinsky & F. Paul Pittman

Pakistan



Saifullah Khan



Saeed Hasan Khan

S. U. Khan Associates Corporate & Legal Consultants

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The legislation on data protection is in draft/Bill stage and yet to be passed by Parliament. Its title is the Personal Data Protection Bill, 2020 (“the Bill”).

1.2 Is there any other general legislation that impacts data protection?

The Prevention of Electronic Crimes Act, 2016 also contains certain significant provisions about data protection.

1.3 Is there any sector-specific legislation that impacts data protection?

Within the banking sector, the Payment Systems and Electronic Funds Transfers Act, 2007 provides for the secrecy of financial institutions’ customer information; violation is punishable with imprisonment or a financial fine, or both. For the telecoms industry, the Telecom Consumer Protection Regulations, 2009 confer on subscribers of telecoms operators the right to lodge complaints for any illegal practices with the Pakistan Telecommunication Authority, “illegal practices” being a broad term which includes, *inter alia*, illegal use of personal data of subscribers.

1.4 What authority(ies) are responsible for data protection?

Under the Bill, the proposed Personal Data Protection Authority of Pakistan would primarily be responsible for data protection.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **“Personal Data”**
“personal data” means 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 anonymized, encrypted or pseudonymized data which is incapable of identifying an individual is not personal data.

- **“Processing”**
“processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **“Controller”**
“Data controller” means a natural or legal person or the government, who either alone or jointly has the authority to make a decision on the collection, obtaining, usage or disclosure of personal data.
- **“Processor”**
“Data processor” means a natural or legal person or the government who, alone or in conjunction with other(s), processes data on behalf of the data controller.
- **“Data Subject”**
“Data subject” means a natural person who is the subject of the personal data.
- **“Sensitive Personal Data”**
“Sensitive personal data” means and includes data relating to access control (username and/or password), financial information such as bank account, credit card, debit card, or other payment instruments, and, passports, biometric data, and physical, psychological, and mental health conditions, medical records, and any detail pertaining to an individual’s ethnicity, religious beliefs, or any other information for the purposes of this Act and rules made thereunder.
- **“Data Breach”**
There is no definition of this term in the Bill.
Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)
- “pseudonymisation” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
- **“Vital interests”** means matters relating to life, death or security of a data subject.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Section 3(2) of the Bill made the Bill applicable to data controllers and processors not registered or established in Pakistan. Such data controllers and processors are required to nominate a representative in Pakistan.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
The principle of transparency is not dealt with in the Bill.
- **Lawful basis for processing**
The collection, processing and disclosure of personal data shall only be done in compliance with the provisions of the Bill. A data controller shall not process personal data including sensitive personal data of a data subject unless the data subject has given his consent to the processing.
- **Purpose limitation**
Personal data shall not be processed unless the processing of the personal data is necessary for, or directly related to, that purpose.
- **Data minimisation**
Personal data shall not be processed unless the personal data are adequate but not excessive in relation to that purpose.
- **Proportionality**
This is not dealt with in the Bill.
- **Retention**
The Bill stipulates that personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose. The Bill confers a duty on the data controller to take all reasonable steps to ensure that all personal data are destroyed or permanently deleted if they are no longer required for the purpose for which they were to be processed.

Other key principles – please specify

- The Bill recognises and provides for consent to be an essential requirement to process personal data of the data subject. The Bill also provides that the data controller may not disclose personal data without the consent of the data subject. The Personal Data Protection Authority is to protect personal data from any loss or misuse, to promote awareness of data protection and to deal with complaints.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
The data subject is granted the right of access to personal data, upon payment of a prescribed fee, as to the data subject's personal data that are being processed by or on behalf of the data controller. The data controller must comply with such data access request within 30 days (extendable to an additional 14 days under certain circumstances).

The data subject is entitled to:

- information as to the data subject's personal data that are being processed by or on behalf of the data controller; and
- have communicated to him a copy of the personal data in an intelligible form.
- **Right to rectification of errors**
In the case that personal data have been supplied to the data subject upon his request and the same are inaccurate, incomplete, misleading or not up to date, or when the data subject knows that his personal data are inaccurate, incomplete, misleading or not up to date, the data subject has the right to get them corrected by making a written request to the data controller.
- **Right to deletion/right to be forgotten**
The data subject has the right to request that the data controller, without undue delay, erase personal data in the following situations:
 - the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - the data subject withdraws the consent on which the processing is based;
 - the data subject objects to the processing;
 - the personal data have been unlawfully processed; or
 - the personal data must be erased for compliance with a legal obligation.
- **Right to object to processing**
The data subject has the right to give "data subject notice" in writing to the data controller to:
 - (i) cease the processing, or processing for a specified purpose or in a specified manner; or
 - (ii) not begin the processing, or processing for a specified purpose or in a specified manner.
 The data subject must state reasons in the "data subject notice" that:
 - (i) the processing of that personal data or the processing of personal data for that purpose or in that manner is causing, or is likely to cause, substantial damage or distress to him or to another person; and
 - (ii) the damage or distress is, or would be, unwarranted.
- **Right to restrict processing**
As explained above.
- **Right to data portability**
There is no such right in the Bill.
- **Right to withdraw consent**
The data subject has the right to withdraw his consent.
- **Right to object to marketing**
The data subject has the right to give "data subject notice" in writing to the data controller to:
 - (i) cease the processing, or processing for a specified purpose or in a specified manner; or
 - (ii) not begin the processing, or processing for a specified purpose or in a specified manner.
 The data subject must state reasons in the "data subject notice" that:
 - (i) the processing of that personal data or the processing of personal data for that purpose or in that manner is causing, or is likely to cause, substantial damage or substantial distress to him or to another person; and
 - (ii) the damage or distress is, or would be, unwarranted.
- **Right to complain to the relevant data protection authority(ies)**
The data subject may file a complaint before the proposed Personal Data Protection Authority of Pakistan against any violation of personal data protection rights as granted

under the Bill, regarding the conduct of any data controller, data processor or their processes which the data subject regards as involving:

- (i) a breach of the data subject's consent to process data;
- (ii) a breach of obligations of the data controller or the data processor in the performance of their functions under the Bill;
- (iii) the provision of incomplete, misleading or false information while taking consent of the data subject; or
- (iv) any other matter relating to protection of personal data.

Other key rights – please specify

- None other than the above.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

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

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

6.6 What are the sanctions for failure to register/notify where required?

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

6.7 What is the fee per registration/notification (if applicable)?

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

6.9 Is any prior approval required from the data protection regulator?

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

6.10 Can the registration/notification be completed online?

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

6.11 Is there a publicly available list of completed registrations/notifications?

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

6.12 How long does a typical registration/notification process take?

This aspect will be addressed under the rules to be framed by the proposed Personal Data Protection Authority of Pakistan (please see question 6.1 above).

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

There is no expressed requirement in the Bill; however, while discussing the power of the Personal Data Protection Authority of Pakistan, the Bill confers upon it the power to formulate responsibilities of the Data Protection Officer. Therefore, the

proposed Personal Data Protection Authority of Pakistan, when established, will devise the registration requirements.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

In view of question 7.1 above, this is not applicable.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

In view of question 7.1 above, this is not applicable.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

In view of question 7.1 above, this is not applicable.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

In view of question 7.1 above, this is not applicable.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

In view of question 7.1 above, this is not applicable.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

In view of question 7.1 above, this is not applicable.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

In view of question 7.1 above, this is not applicable.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The Bill is silent on this aspect; however, businesses customarily execute an agreement to this effect.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

It is not necessary, under the Bill, to enter into an agreement. However, for the enforcement of an agreement, such formalities must be summarised in writing and registered under the Registration Act, 1908.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

No such legislative restriction exists.

9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

No such legislative restriction exists.

9.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

No such legislative restriction exists.

9.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

No such legislative restriction exists.

9.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

A data protection authority, for the time being, is non-existent.

9.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

There is no law regulating this mechanism as such.

9.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

There are none, as there is no legislation to this effect.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

No such legislative restriction exists.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

No such legislative restriction exists.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

None, in view of there not being any legislation to this effect, and the fact that no data protection authority exists.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

None, in view of there not being any legislation to this effect.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The 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 protection provided under the Bill. The personal data so transferred shall be processed in accordance with the 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 this requirement on the grounds of necessity or strategic interests.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

There are no such mechanisms.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

This is not yet specified in the Bill, although it may be a subject matter of the rules to be framed thereunder.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Public Interest Disclosures Act, 2017 deals with the concept of “whistler-blowers”; however, the same primarily deals with and focuses on public sector entities. The said Act has mandated the Government to specify private sector entities (in the official *Gazette*) to be an “organization” for the purposes of said Act. Primarily, the Public Interest Disclosures Act, 2017

covers the wilful misuse of power or wilful misuse of discretion by virtue of which substantial loss is caused to the Government or substantial wrongful gain accrues to a public servant or to a third party. As such, the corporate sector is not the subject matter of the Public Interest Disclosures Act, 2017.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous or pseudonymous disclosures are not entertained in terms of Section 3(5) of the Public Interest Disclosures Act, 2017.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

There exists no legislation that requires registration/notification or prior approval for using CCTV.

13.2 Are there limits on the purposes for which CCTV data may be used?

There are no such limits (please see question 13.1 above).

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

There is no law related to this subject.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

As there is no law, there is no legislative requirement to obtain consent; however, consent is generally built-in within the employment contract.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no such requirement.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Data controllers, under the Bill, are responsible for taking practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The Bill requires the data controller to report a data breach to the Personal Data Protection Authority of Pakistan within 72 hours. The exception is where the personal data breach is unlikely to result in a risk to the rights and freedoms of the data subject.

In case the notification is made beyond 72 hours, the notification is to state reasons for the delay.

The notification must contain the following information:

- Description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
- Name and contact details of the Data Protection Officer or other contact point where more information can be obtained.
- Likely consequences of the personal data breach.
- Measures adopted or proposed to be adopted by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

There is no such requirement in the Bill.

15.4 What are the maximum penalties for data security breaches?

Breach	Penalty
Anyone who processes or causes to be processed, disseminates or discloses personal data in violation of this Act.	Fine of up to PKR 15 million (US\$ 90,000 approx.) and in case of a subsequent unlawful processing or in case of sensitive data, the fine may be increased up to PKR 25 million (US\$ 150,000 approx.).
Failure to adopt the security measures that are necessary to ensure data security.	Fine of up to PKR 5 million (US\$ 30,000 approx.).
Failure to comply with the orders of the Personal Data Protection Authority of Pakistan or the court.	Fine of up to PKR 5 million (US\$ 30,000 approx.).
Corporate liability on a legal person.	Fine not exceeding 1% of its annual gross revenue in Pakistan or PKR 30 million (US\$ 180,000 approx.), whichever is greater.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Investigatory/ Enforcement Power	Civil/Administrative Sanction	Criminal Sanction
Complaint redressal.	To seek information from the data controller or data processor.	N/A
Decide the complaint.	Imposition of penalties.	N/A
Enforcement of orders.	In the case that the data controller or data processor fails to execute the order, the proposed Personal Data Protection Authority of Pakistan may initiate enforcement proceedings.	N/A

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The Bill is silent on this.

16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

As the Personal Data Protection Authority of Pakistan is not in existence, there is nothing to state regarding its approach, nor any cases as yet.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

This is not applicable (please see question 16.3 above).

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The Bill is silent on this aspect; however, generally the foreign law enforcement agencies do not communicate with businesses directly; rather, businesses are contacted via the relevant law enforcement agencies of Pakistan, who coordinate with businesses to respond to foreign law enforcement agencies.

17.2 What guidance has/have the data protection authority(ies) issued?

No such guidelines exist.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Recently, Pakistani bank data were the subject of a cyber-attack, with customers receiving notifications about money transfers from their account. Following various abnormal international transactions and complaints from customers, the affected bank immediately reacted and shut down its system to stop further transactions. This timely action helped keep losses to PKR 2.6 million, as opposed to a potential PKR 5 million to 6 million. Currently, the State Bank of Pakistan and relevant agencies are investigating the incident. Pakistan's Prevention of Electronic

Crimes Act, 2016 has already made unauthorised interference with information systems and transmission of data a criminal offence. Moreover, the State Bank of Pakistan has directed all banks to take steps to identify and counter any cyber threat to their IT systems in coordination with international payment schemes.

18.2 What "hot topics" are currently a focus for the data protection regulator?

As stated above, a Personal Data Protection Authority of Pakistan is non-existent for the time being; however, once it comes into being, e-Commerce, banking transactions and cellular data are certainly among the "hot topics" on which the Authority is expected to focus.



Saifullah Khan is an international trade lawyer, with 20 years' experience in international trade policy and law advisory, serving foreign and Pakistani clients. His practice areas include International Trade Advisory related to World Trade Organization laws on Trade Remedies, GATS and TRIPS etc., Competition Law, Privacy & Personal Data Protection, E-commerce Regulatory Framework, Arbitration and Investment advisory. He has advised the Government of Pakistan on the amendment of trade defence laws and rules, the e-Commerce Policy Framework and also assisted the Federal Board of Revenue (Pakistan National Tax Administration) in its drafting of the law on the "Pakistan Single Window". He attended the 50th session of the United Nations Commission on International Trade Law as the "Alternate Pakistan Representative", wherein the Model Law on Electronic Transferable Records was adopted. Mr. Khan is an Advocate of the High Court, a Fellow Member of the Institute of Cost & Management Accountants of Pakistan and a Member of the Chartered Institute of Arbitrators (UK).

S. U. Khan Associates Corporate & Legal Consultants
 First Floor, 92 Razia Sharif Plaza
 Fazal-ul-Haq Road, Blue Area
 Islamabad, 44000
 Pakistan

Tel: +92 51 23447 41/42
 Email: saifullah.khan@sukhan.com.pk
 URL: www.sukhan.com.pk



Saeed Hasan Khan is a tax practitioner with experience in all three tiers of taxation services (advisory, compliance and litigation), in both direct and indirect taxes. He also has good working experience of the Companies Act, 2017 (formerly the Companies Ordinance, 1984), dealing with company incorporation and matters related thereto. His other practice areas include Labour and Trade Organization laws. He has a good command over VAT law and practice of the United Arab Emirates. He also practises Data Protection, e-Commerce and IT law. Mr. Khan is an Advocate of the High Court, an Affiliate of the Institute of Chartered Accountants of Pakistan, and a Member of the Chartered Institute of Arbitrators (UK).

S. U. Khan Associates Corporate & Legal Consultants
 First Floor, 92 Razia Sharif Plaza
 Fazal-ul-Haq Road, Blue Area
 Islamabad, 44000
 Pakistan

Tel: +92 51 23447 41/42
 Email: saeed.hasan@sukhan.com.pk
 URL: www.sukhan.com.pk

S. U. Khan Associates Corporate & Legal Consultants is a pioneering and leading firm practising trade remedy law, with local and international clients. The major service areas include International Trade Consultancy, Anti-Trust Law Consultancy, Data Protection, e-Commerce & IT Laws, Competition Law, International Trade Development, Foreign Investment Advisory Services, International Trade Agreements (FTAs, PTAs and SAFTA) Advisory, International Trade Management, Industry & Market Research, etc. The Firm is also a great contributor to the dissemination of professional knowledge in various journals and national and international institutions, such as the United Nations Conference on Trade and Development and the World Trade Organization. The Firm now has a presence and an establishment in Dubai, United Arab Emirates.

www.sukhan.com.pk



S.U.Khan Associates
 Corporate & Legal Consultants

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs

Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law

Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms