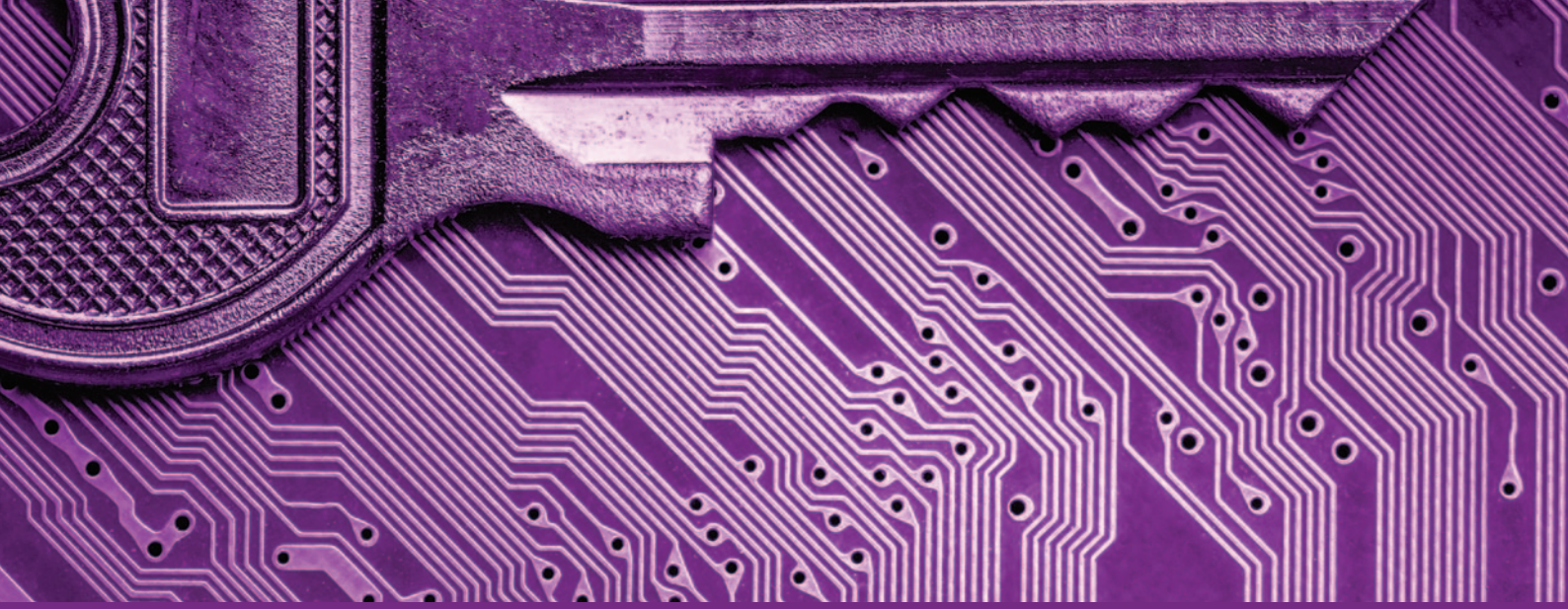

ICLG

The International Comparative Legal Guide to:

Data Protection 2019

6th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Addison Bright Sloane
Anderson Mōri & Tomotsune
Ashurst Hong Kong
Assegaf Hamzah & Partners
BEITEN BURKHARDT
Bird & Bird
Christopher & Lee Ong
Çiğdemtekin Çakırca Arancı Law Firm
Clyde & Co
Cuatrecasas
Deloitte Legal Shpk
DQ Advocates Limited
Drew & Napier LLC
Ecija Abogados
FABIAN PRIVACY LEGAL GmbH
GANADO Advocates
Herbst Kinsky Rechtsanwälte GmbH
Herzog Fox & Neeman
Infusion Lawyers
Integra Law Firm
KADRI LEGAL
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys At Law
Lee & Ko
LPS L@w
Lydian
Matheson
Mori Hamada & Matsumoto
Morri Rossetti e Associati Studio Legale e Tributario
Nyman Gibson Miralis
OLIVARES
Osler, Hoskin & Harcourt LLP
Pestalozzi Attorneys at Law
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Rothwell Figg
S. U. Khan Associates Corporate & Legal Consultants
Subramaniam & Associates (SNA)
thg IP/ICT
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg global legal group

global legal group

Contributing Editor
Tim Hickman &
Dr. Detlev Gabel,
White & Case LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Nicholas Catlin

Senior Editors
Caroline Collingwood
Rachel Williams

CEO
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
June 2019

ISBN 978-1-912509-76-8
ISSN 2054-3786

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Continued Overleaf

global legal group

Country Question and Answer Chapters:

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 the Parliament. Its title is the Personal Data Protection Bill 2018 ("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 Consumers Protection Regulations, 2009 confers 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 National Commission for Personal Data Protection 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 in respect of commercial transactions, which:

  (i) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;

  (ii) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or

  (iii) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

  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 and expression of opinion about the data subject.

- "**Processing**"

  "Processing", in relation to personal data, means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including:

  (i) the organisation, adaptation or alteration of personal data;

  (ii) the retrieval, consultation or use of personal data; and

  (iii) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or

  (iv) the alignment, combination, correction, erasure or destruction of personal data.

- "**Controller**"

  "Data controller" means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorises the processing of any personal data, but does not include a data processor.

- "**Processor**"

  "Data processor", in relation to personal data, means any person, other than an employee of the data user, who processes the personal data solely on behalf of the data controller, and does not process the personal data for any of his own purposes.

- "**Data Subject**"

  "Data subject" means an individual who is the subject of the personal data.

- "**Sensitive Personal Data**"

  "Sensitive personal data" means personal data revealing racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership in political parties, trade unions, organisations and associations with a religious, philosophical, political or trade-union, or provide information as to the health or sexual life of an individual, or the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have

been committed by him, or the disposal of such proceedings or the sentence of any court in such proceedings or financial, or proprietary confidential personal data; OR

"sensitive personal data" means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Commission may determine by order published in the Gazette.

- "**Data Breach**"

  There is no definition of this term in the relevant national legislation.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  "Commercial transaction" means any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance.

  "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)(b) of the Bill brought the applicability of the Bill on businesses (persons) not established in Pakistan but using equipment in Pakistan for processing personal data otherwise than for the purposes of transit through Pakistan. Those persons are required to nominate a representative in Pakistan for the purposes of the Bill.

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**

  Personal data shall not be processed unless the personal data are processed for a lawful purpose directly related to an activity of the data controller.

- **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 data controller is further required to take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

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, and the data controller with information as to the data subject's personal data that are being processed by or on behalf of the data controller, must comply with such data access request within 21 days. 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 is inaccurate, incomplete, misleading or not up to date, or when the data subject knows that his personal data are so inaccurate, incomplete, misleading or not up to date, the data subject has the right to get it 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 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 have to 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 has to 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 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 of the data or their processing for a specified purpose or in a specified manner; or

  (ii) not begin the processing of the data or their processing for a specified purpose, or in a specified manner.

  The data subject has to 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 National Commission for Personal Data Protection 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 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 are no such requirements in the Bill; however, the Bill confers upon the Federal Government powers for rule-making. It is expected that after the promulgation of the law, the Federal Government, in the exercise of its rule-making powers, will notify such procedural 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 Federal Government (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 Federal Government (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 Federal Government (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 Federal Government (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 Federal Government (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 Federal Government (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 Federal Government (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 Federal Government (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 Federal Government (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 Federal Government (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 Federal Government (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.

The Bill does not have a requirement for the appointment of a Data Protection Officer, either mandatory or optional.

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 need to 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 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.

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

No such legislative restriction exists.

9.4 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.

9.5 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.

9.6 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.

No such legislative restriction exists.

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, in view of there not being any legislation to this effect.

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 required, as there is no legislation to this effect.

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 the 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 the 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 National Commission for Personal Data Protection has powers to seek information from the data controller in respect of data processing; however, as the said Commission is not yet in existence, there have not been any rules issued on this matter.

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?

The National Commission for Personal Data Protection has powers to impose penalties for non-compliance and non-observance of data security practices; however, as the said Commission is not yet in existence, there is no quantification of such penalties.

16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Complaint redressal.	To seek information from data controllers.	Direction to local police to file a case with the Court.
N/A	Imposition of penalties.	N/A
N/A	To order a data controller to take such reasonable measures as it may deem necessary to remedy an applicant for any failure to implement the provisions of the Bill.	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 National Commission for Personal Data Protection has powers to order a data controller to take such reasonable measures as it may deem necessary, which may include a ban; however, as the said Commission is not in existence, procedural aspects in relation to having an order from the Court, etc., are uncertain at the moment.

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

As the National Commission for Personal Data Protection 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 notification 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 Rs 2.6m as opposed to Rs 5m to 6m. Currently, the State Bank of Pakistan and relevant agencies are investigating the incident. Pakistan's Prevention of Electronic Crime 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 National Commission for Personal Data Protection is not 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 said Commission is expected to focus.

Saifullah Khan

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

Mr. Saifullah Khan is an international trade lawyer, with 20 years' experience in international trade policy and law advisory, serving foreign and Pakistani clients. He has also advised the Pakistani government on the amendment of trade defence laws and rules. Furthermore, Mr Khan has an extensive global advisory portfolio in international trade management systems, international trade agreements and para-tariff and non-tariff barrier issues. Mr. Khan has also gained experience in policy and regulatory frameworks regarding e-Commerce. He is an Advocate of the High Court, a Fellow Member of the Institute of Cost & Management Accountants (ICMAP) and the Pakistan Institute of Public Finance Accountants (PIPFA), a Certified Internal Auditor (USA) and Member of the Chartered Institute of Arbitrators (UK), and recently attended an executive education programme at Harvard University, USA on Mastering Trade Policy.

Saeed Hasan Khan

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

Mr. Saeed Hasan Khan is a tax practitioner with experience at all three tiers of taxation services (advisory, compliance and litigation), both in 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. He is an Advocate of the High Court, an Affiliate of the Institute of Chartered Accountants of Pakistan, a Fellow Member of the Pakistan Institute of Public Finance Accountants (PIPFA), and a Member of the Chartered Institute of Arbitrators (UK).

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- Fintech
- 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
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com