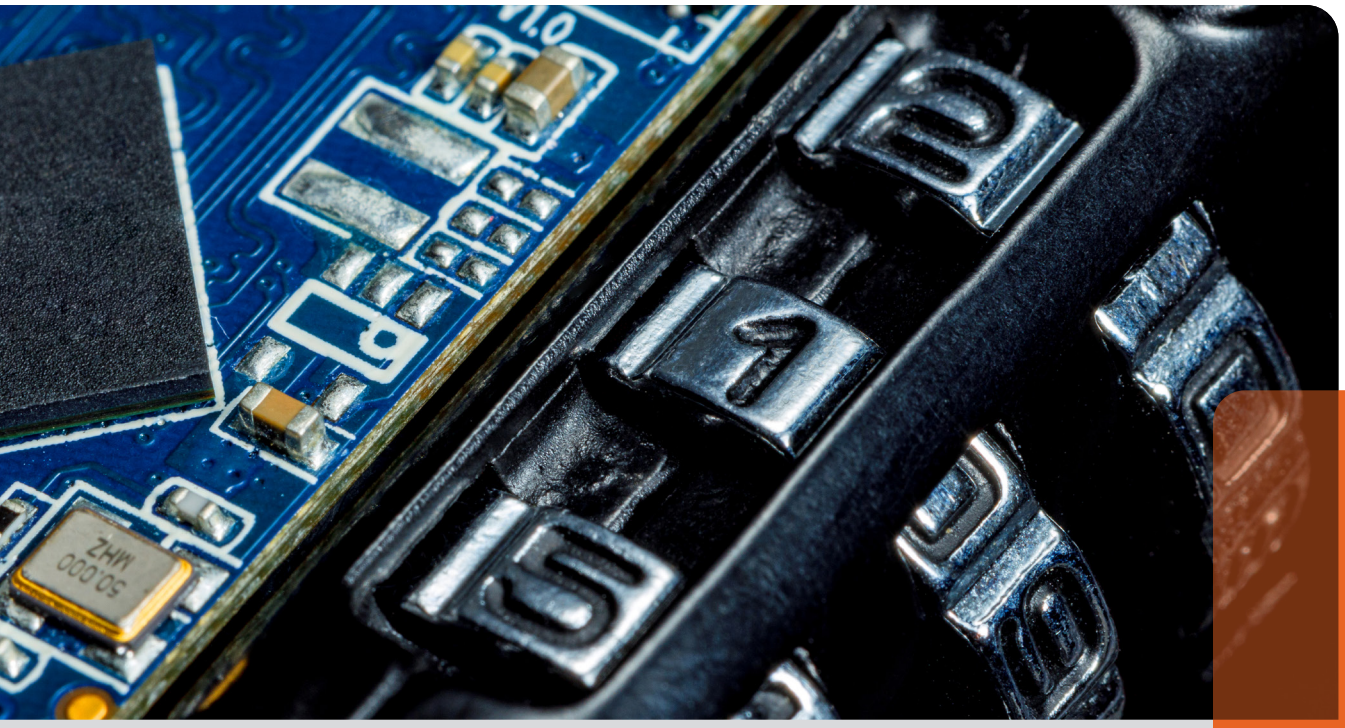
International
Comparative
Legal Guides



# Data Protection

# 2024

11th Edition

Contributing Editors:
Tim Hickman & Detlev Gabel
White & Case LLP

glg Global Legal Group

# Expert Analysis Chapters



# Q&A 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 Parliament. Its title is the Personal Data Protection Bill, 2023 ("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 ("PTA"), "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 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.
  Anonymised, encrypted or pseudonymised 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**"
  "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**"
  "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**"/"**Special Categories of Personal Data**"
  "Sensitive personal data" means and includes: financial information, including identification number, credit card data, debit card data, account number or other payment instrument data; health data, including physical, behavioural, psychological and mental health conditions or medical records; computerised national ID card or passport; biometric data; genetic data; religious beliefs; criminal records; political affiliations; caste or tribe; and the individual's ethnicity.
- "**Data Breach**"
  A "Personal Data Breach" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.
- **Other Key Definitions**
  - "Pseudonymisation" is 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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

- "Vital interests" means matters relating to life, fundamental rights, security of a data subject(s), humanitarian emergencies, in particular in situations of natural and man-made disasters, monitoring and management of epidemics.
- "Critical personal data" means such personal data retained by the public service provider – excluding data open to the public. It also includes data identified by sector regulators and classified by the commission as critical and also any data related to international obligations.
- "Significant" means any data controller or processor that is sufficiently great or important to be worthy of attention by its sales revenue, profit, number of employees, market share, capital employed, or any other indicator such as number of users, type of data collected or a combination thereof that may constitute it as significant.

## 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?

The Bill is applicable to data controllers and processors not incorporated in Pakistan (operating digitally or non-digitally in Pakistan) and involved in commercial or non-commercial activity. The Bill is also applicable to data controllers and processors who have no physical appearance in Pakistan but carry out the processing of personal data in a territory where Pakistani law is applicable under public or private international law.

### 3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The Bill does not specify any processing activities that are out of the Bill's material scope; however, it has specified the cases where the processing shall be within the scope of the personal data protection Bill, 2023. The Bill shall be applicable to those data controllers and processors that:

- Are established/registered/present in Pakistan and are processing or authorising the processing of the personal data.
- Have digital presence in Pakistan and are involved in the processing of the personal data concerning any commercial or non-commercial activity but are incorporated outside Pakistan in any other jurisdiction.
- Have no physical presence in Pakistan but are processing personal data of individuals in territories where Pakistani Law is applicable under public and private international law.
- Collect the personal data of data subjects within 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 carried out in compliance with the provisions of the Bill. Personal data shall not be processed unless processed for a lawful purpose directly related to an activity of the data controller (lawful purpose).
- **Purpose limitation**
  Personal data shall not be processed unless the processing of the personal data is necessary for, or directly related to, lawful purpose.
- **Data minimisation**
  Personal data shall not be processed unless the personal data is adequate; however, the personal data must not be excessive in relation to lawful 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.
- **Accuracy**
  The Bill confers this obligation upon the Data Controller that it must take such adequate steps which must ensure the accuracy of the personal data processed. The Bill makes it obligatory for the Controller to make sure that data processed must be accurate, complete and not misleading and must be kept up to date.
- **Other key principles**
  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 for any purpose other than the purpose for which the same was to be disclosed at the time of collection or to any third party not earlier notified. The Personal Data Protection Authority protects personal data from any loss or misuse, promote awareness of data protection and deal with complaints. The data controllers/processors who are to be identified as "significant" by the Commission are required to appoint a Data Protection Officer for the sake of the processing of the personal data.

## 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/information about processing**
  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 within 14 days, 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**
  The data subjects have the right to data portability.
- **Right to withdraw consent**
  The data subject has the right to withdraw his consent.
- **Right protecting against solely automated decision-making and profiling**
  The data subject has the right to not be subjected to automated decision-making, including profiling.
- **Right to complain to the relevant data protection authority(ies)**
  The data subject may file a complaint before the proposed National Commission for Personal Data Protection 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.

**5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.**

There is no such right in the Bill.

## 6 Children's Personal Data

**6.1 What additional obligations apply to the processing of children's personal data?**

The data controller or processor shall process a child's personal data in such a manner that protects the rights and interests of the child:

- before processing any personal data relating to a child, a data controller or processor must verify the child's age;
- seek consent of the child's parent, relevant person or authorised person having parental responsibility over the child to decide on his behalf;
- not process any personal data of a child that is likely to cause the child harm; and
- not subject the child to tracking, behavioural monitoring or targeted advertising.

## 7 Registration Formalities and Prior Approval

**7.1 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 express requirement in the Bill; however, while discussing the power of the National Commission for Personal Data Protection of Pakistan, the Bill confers upon it the power to devise a registration mechanism for data controllers and data processors. Therefore, the proposed National Commission for Personal Data Protection of Pakistan, when established, will devise the registration requirements. The data controller and data processor, whether digitally or non-digitally operational within the territory of Pakistan, must register with the proposed National Commission for Personal Data Protection of Pakistan in such manner as may be specified by the registration framework to be formulated by the proposed Commission.

Those data controllers and/or data processors who are already registered with any public body shall only be required to intimate the Commission about data processing.

**7.2 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 National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

**7.3 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 National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

**7.4 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 National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

**7.5 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 National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

**7.6 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 National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

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

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

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

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

**7.9 Is any prior approval required from the data protection regulator?**

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

**7.10 Can the registration/notification be completed online?**

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

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

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

**7.12 How long does a typical registration/notification process take?**

This aspect will be addressed under the rules to be framed by the proposed National Commission for Personal Data Protection of Pakistan (please see question 7.1 above).

## 8 Appointment of a Data Protection Officer

**8.1 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 data controller and/or data processor identified as "significant" by the Commission shall be required to appoint a Data Protection Officer. A Data Protection Officer needs to be well versed in the collection and processing of personal data and the risks associated with the processing.

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

There is no specific provision regarding this; however, whosoever shall process any personal data in violation of the provisions of the Bill shall be punished with a fine of up to 125,000 USD or an equivalent amount in Pakistani Rupees.

**8.3 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?**

The Bill is silent on this aspect. It is expected that further guidelines, in this regard, will be provided under the Rules to be framed by the Commission.

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

The Bill is silent on this aspect. It is expected that further guidelines, in this regard, will be provided under the Rules to be framed by the Commission.

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

No qualifications are prescribed in the Bill. It is expected that further guidelines, in this regard, will be provided under the Rules to be framed by the Commission.

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

The Bill is silent on this aspect. It is expected that further guidelines, in this regard, will be provided under the Rules to be framed by the Commission.

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

The Bill is silent on this aspect. It is expected that further guidelines, in this regard, will be provided under the Rules to be framed by the Commission.

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

The Bill is silent on this aspect. It is expected that further guidelines, in this regard, will be provided under the Rules to be framed by the Commission.

## 9 Appointment of Processors

**9.1 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.

**9.2 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.

## 10 Marketing

**10.1 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?).**

The Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations, 2009, (administered by the PTA) require that all operators (telecom operators licensed by the PTA) establish a standard operating procedure to control spamming. Similarly, all such operators are required to develop a standard operating procedure for controlling unsolicited calls. The operators are also required to establish a consolidated "Do Not Call Register" in connection with controlling unsolicited calls. The operators are further required to ensure registration of telemarketers.

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

As discussed at question 10.1 above.

**10.3 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.).**

As discussed at question 10.1 above.

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

The restrictions discussed at question 10.1 only apply to operators in Pakistan being licensed by the PTA.

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

The PTA is entrusted with monitoring and enforcement as explained at question 10.1 above.

**10.6 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.

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

Contravention of the Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations, 2009, is an offence under the PTA (Re-organization) Act, 1996, punishable with imprisonment which may extend to three years or a fine which may extend to PKR 10 million, or both.

## 11 Cookies

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

The Bill gives the right to data subjects to not be subject to a decision solely based upon automated processing, including profiling.

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

The Bill does not distinguish between types of cookies.

**11.3 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.

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

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

## 12 Restrictions on International Data Transfers

**12.1 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 the Government of 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. Another basis to transfer data outside is consent of the data subject. Thirdly, personal data may also be transferred outside Pakistan under a framework to be devised by the National Commission for Personal Data Protection of Pakistan. The personal data so transferred shall be processed in accordance with the Bill. Critical personal data shall only be processed in Pakistan.

In the absence of an adequate level of protection, the National Commission for Personal Data Protection of Pakistan may allow the transfer of personal data outside Pakistan as follows:

- Under a binding contract/agreement.
- With the explicit consent of the data subject that has no conflict with the public or national interest of Pakistan.
- International cooperation under any relevant international obligation.
- On conditions to be specified by the National Commission for Personal Data Protection of Pakistan.

**12.2 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.).**

As the law on personal data protection is not yet enforced, businesses typically transfer personal data on the basis of contractual arrangements.

**12.3 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.

**12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.**

The Bill is silent on transfer impact assessment.

**12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

This is not applicable.

**12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?**

As the National Commission for Personal Data Protection of Pakistan is not in existence, no such guidance exists.

## 13 Whistle-blower Hotlines

**13.1 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 Bill does not have any provision related to "whistle-blowers". The Public Interest Disclosures Act, 2017, deals with the concept of "whistler-blower"; 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 "organisation" 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 covered by the Public Interest Disclosures Act, 2017.

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

The Bill is silent on this matter; however, anonymous or pseudonymous disclosures are not entertained in terms of Section 3(5) of the Public Interest Disclosures Act, 2017.

## 14 CCTV

**14.1 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)?**

The Bill does not place or require any registration/notification or prior approval in relation to the use of CCTV.

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

There are no such limits (please see question 14.1 above).

## 15 Employee Monitoring

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

The Bill does not have any provision regarding employee monitoring.

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

The Bill does not have such requirement. However, consent is generally built-in within the employment contract.

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

There is no such requirement.

**15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?**

The Bill is silent on this aspect of personal data processing.

## 16 Data Security and Data Breach

**16.1 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.

**16.2 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 National Commission for Personal Data Protection 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 after 72 hours, the notification must state the 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.

**16.3 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.**

The reporting requirements for the data subjects are the same as explained at question 16.2.

**16.4 What are the maximum penalties for personal data security breaches?**

| Breach | Penalty |
|---|---|
| A data controller not ceasing the processing of personal data after withdrawal of consent by the data subject. | Fine of 50,000 USD or an equivalent amount in Pakistani Rupees. |
| Anyone who processes or causes to be processed, disseminates or discloses personal data in violation of this Act. | Fine of up to 125,000 USD or an equivalent amount in Pakistani Rupees, and in case of a subsequent unlawful processing the fine may be raised up to 250,000 USD or an equivalent amount in Pakistani Rupees. In the case of sensitive personal data, the fine is up to 500,000 USD or an equivalent amount in Pakistani Rupees, while, where the offence is related to critical personal data the fine is up to 1 million USD or an equivalent amount in Pakistani Rupees. |
| Failure to adopt the security measures that are necessary to ensure data security. | Fine of up to 50,000 USD or an equivalent amount in Pakistani Rupees. |
| Failure to comply with the orders of the National Commission for Personal Data Protection of Pakistan or the court. | Fine of up to 50,000 USD or an equivalent amount in Pakistani Rupees. |
| Failure to comply with the directions of the National Commission for Personal Data Protection of Pakistan. | Fine of up to 2 million USD or an equivalent amount in Pakistani Rupees.<br>Suspension or termination of the registration and impose additional conditions. |
| Corporate liability. | Fine of up to 200,000 USD or 1% of annual gross revenue, whichever is higher. |

## 17 Enforcement and Sanctions

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

(a) **Investigative Powers**: The National Commission for Personal Data Protection of Pakistan shall have the powers to decide a complaint, under the Bill, and shall be deemed to be a Civil Court and shall have the same powers as are vested in a Civil Court.

(b) **Corrective Powers**: The National Commission for Personal Data Protection of Pakistan shall have the powers 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. In addition, it shall have the powers to take prompt and appropriate action in response to a data security breach.

(c) **Authorisation and Advisory Powers**: Advising the Federal Government and any other statutory authority on measures that must be undertaken to promote protection of personal data and ensuring consistency of application and enforcement of the Bill shall be one of the functions entrusted to the National Commission for Personal Data Protection of Pakistan.

(d) **Imposition of administrative fines for infringements of specified legal provisions**: As discussed in question 16.4.

(e) **Non-compliance with a data protection authority**: The National Commission for Personal Data Protection of Pakistan shall have the power to impose a fine of up to 50,000 USD or an equivalent amount in Pakistani Rupees in case anyone fails to comply with its orders. In case of non-compliance with its directions, the fine can be up to 2 million USD or an equivalent amount in Pakistani Rupees.

**17.2 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.

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

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

**17.4 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 17.3 above).

## 18 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**18.1 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.

**18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?**

As the National Commission for Personal Data Protection of Pakistan is not in existence, no such guidelines exist.

## 19 Trends and Developments

**19.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.**

There are no enforcement trends that have emerged in Pakistan over the last 12 months.

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

As the National Commission for Personal Data Protection of Pakistan is not yet in existence, once it comes into force, e-Commerce, banking transactions and telecoms are likely to be the "hot topics" on which the authority is expected to focus.

**Saifullah Khan** is an international trade, IT and policy lawyer with more than 20 years of diversified and multi-jurisdictional professional experience serving a large client base in the domestic and international markets. His areas of interest include trade remedy laws of the World Trade Organization, customs law, competition law and data privacy. With respect to emerging discipline of data privacy, he advises clients from different jurisdictions on data privacy compliance and cross-border transfer of data. Additionally, he assists clients in the preparation and review of privacy policies and intra-group agreements concerning cross-border transfer of personal data, etc. He is an advocate of the High Court, a member of the Chartered Institute of Arbitrators (UK) and a member of the International Association of Privacy Professionals. He has completed a course at the London School of Economics and Political Science on "Data: Law, Policy and Regulation".

**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
LinkedIn: www.linkedin.com/in/saifullahkhan

**Saeed Hasan Khan** has vast experience advising clients on various issues such as taxation, corporate, regulatory compliance, contractual obligations etc. and representing them before the authorities. Over the past 20 years, he has practised in direct and indirect taxes, which encompasses all three practice tiers: advisory; execution; and litigation. He advises on cross-border transactions, international tax treaties and matters related to tax due diligence, corporate structures, shareholder agreements and contractual stipulations between the companies. He has developed a keen professional interest in emerging laws about personal data protection and has gained a deep understanding of underlying concepts and principles governing the global data protection laws including the General Data Protection Regulation of the European Union.
He carried out a great deal of research on personal data protection laws in various jurisdictions to have a comparison of core legal principles in various jurisdictions. He attended a course at the London School of Economics and Political Science on "Data: Law, Policy and Regulation". He is an Advocate of the High Court, a Member of the Chartered Institute of Arbitrators (UK) and a Member of the International Association of Privacy Professionals.

**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
LinkedIn: www.linkedin.com/in/saeed-hasan-khan-1338a63a

S. U. Khan Associates Corporate & Legal Consultants is a pioneering and leading firm practising trade remedy law in Pakistan, with local and international clients. The major service areas include International Trade Law, Data Protection & e-Commerce & IT Law, Competition Law, Foreign Investment Advisory Services, and International Trade Agreements Advisory. The Firm is also a great contributor of professional knowledge to various journals as well as international institutions, such as the United Nations Conference on Trade and Development and the United Nations Commission on International Trade Law (UNCITRAL), etc. The partners have been working closely with the Government in drafting legislations and in policy-making.

**www.sukhan.com.pk**

S.U.Khan Associates
Corporate & Legal Consultants

# International Comparative Legal Guides

The **International Comparative Legal Guide** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

**Data Protection 2024** includes two expert analysis chapters and 31 Q&A jurisdiction chapters covering key issues, including:

- Relevant Legislation and Competent Authorities
- Definitions
- Territorial and Material Scope
- Key Principles
- Individual Rights
- Children's Personal Data
- Registration Formalities and Prior Approval
- Appointment of a Data Protection Officer
- Appointment of Processors
- Marketing
- Cookies
- Restrictions on International Data Transfers
- Whistle-blower Hotlines
- CCTV
- Employee Monitoring
- Data Security and Data Breach
- Enforcement and Sanctions
- E-discovery/Disclosure to Foreign Law Enforcement Agencies
- Trends and Developments

The International Comparative Legal Guides are published by: glg Global Legal Group