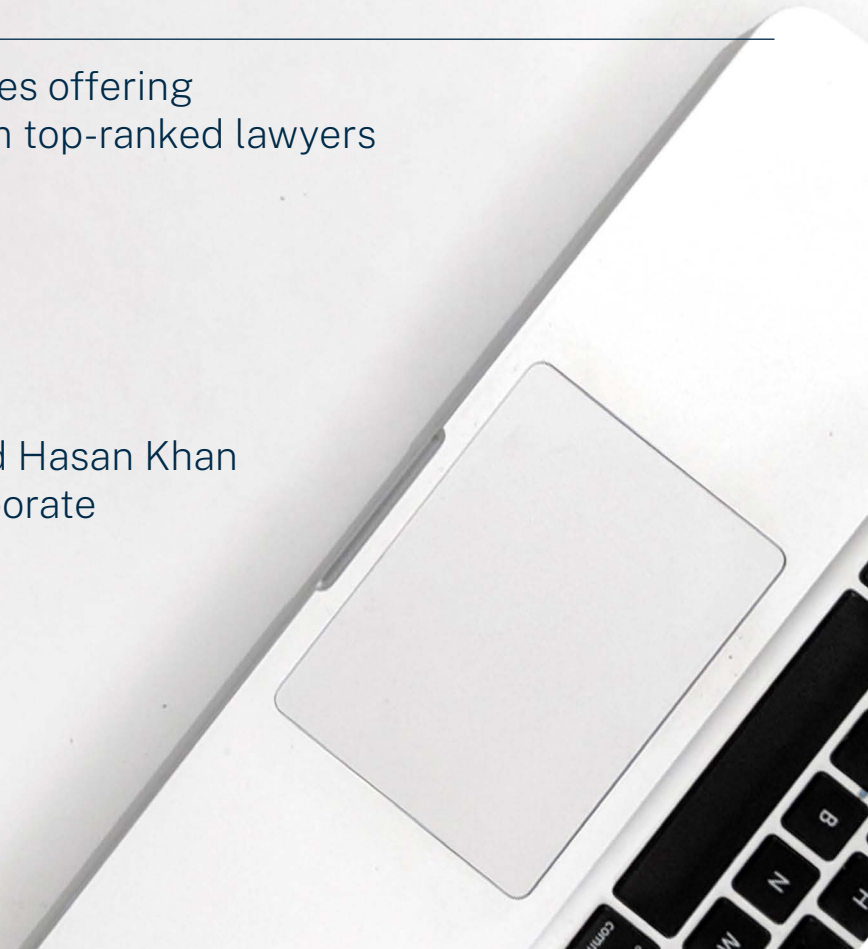
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2024

Definitive global law guides offering comparative analysis from top-ranked lawyers



Pakistan: Law & Practice

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

PAKISTAN

Law and Practice

Contributed by:
Saifullah Khan and Saeed Hasan Khan
S.U.Khan Associates Corporate & Legal Consultants

Contents

S.U.Khan Associates Corporate & Legal Consultants is a pioneering and leading firm practising trade remedy law in Pakistan, with local and international clients. Its major service areas include international trade laws, data protection, e-commerce and IT laws, competition law, customs and taxation, corporate, foreign investment advisory services and international trade agreements advisory. The firm is also a great contributor to the dissemination of professional knowledge in 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). S.U.Khan Associates' partners have been working closely with the government of Pakistan in drafting legislation and in policy-making. The firm advises clients on compliance requirements related to personal data protection, preparation and review of policies and agreements concerning data privacy and transfer of data.

Authors

Saifullah Khan is an international trade, IT and policy lawyer, and has 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 the emerging discipline of data privacy, he advises clients from different jurisdictions about data privacy compliance and cross-border transfer of data. 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.

Saeed Hasan Khan has more than 20 years' experience in advising and representing clients on issues such as taxation, corporate, regulatory compliance and contractual obligations. Mr Khan has developed a keen professional interest in emerging laws on personal data protection, and has gained an understanding of the underlying concepts and principles governing global data protection laws, including the EU's General Data Protection Regulation. He has carried out a great deal of research on personal data protection laws in various jurisdictions. 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
Pakistan

Tel: +92 51 2344 741
Fax: +92 51 2344 743
Email: sukhan@sukhan.com.pk
Web: www.sukhan.com.pk

1. Basic National Regime

1.1 Laws

Privacy, under the Constitution of Pakistan, is an inalienable and fundamental right. Pakistan is developing a specific law on protection of personal data of individuals. The Ministry of Information Technology and Telecommunication (the "Ministry") has developed a draft Personal Data Protection Bill, 2023 (the "draft Bill"). The draft Bill has passed the consultation stage and, after procedural formalities, will be tabled before the legislature for passing into law.

The draft Bill largely follows the General Data Protection Regulation (GDPR) of the European Union.

Sectoral specific laws and regulations exist to safeguard personal information. The Banking Companies Ordinance, 1962 (the "Banking Ordinance") governs the banking sector in Pakistan. The Banking Ordinance provides for the secrecy of information of the customers of the banks. The State Bank of Pakistan (SBP), being the central bank of Pakistan, monitors and implements the secrecy obligations of the banks under the Banking Ordinance.

The Payment Systems and Electronic Fund Transfers Act, 2007 (the "Electronic Funds Transfer Act") regulates electronic fund transfers and protection of the consumer, including the consumer's secrecy and privacy. The SBP has issued regulations in this regard.

The Credit Bureaus Act, 2015, and the regulations made thereunder, govern the unauthorised access or disclosure of credit information.

The Pakistan Telecommunication Authority (PTA) under the PTA (Re-organization) Act, 1996 is empowered to make regulations concerning the telecoms sector, including protection of telecoms consumers. The PTA has issued various regulations, including those related to consumer protection, which ensure the privacy of telecoms consumers.

The Prevention of Electronic Crimes Act, 2016 (PECA) governs unauthorised acts with respect to information systems and provides for related offences. The PECA recognises unauthorised

disclosure of personal information (by relevant service providers) of any person as an offence.

The Right of Access to Information Act, 2017 governs the general public's right to have access to information. Under the Act, any person may make an application for access to information held by a public body. However, any information which would involve invasion of privacy of an identifiable individual is exempt from disclosure under the Right of Access to Information Act.

The Pakistan Information Commission (under the Right of Access to Information Act), while deciding an appeal (No 1080-5-2021 dated 15 September 2021 related to provision of certain information about a housing scheme), has directed the respondent in the appeal to provide the appellant all the requested information after removing the information touching upon the privacy of other members – ie, their addresses, phone numbers, identity cards and bank account numbers or the detail of their family members.

The Ministry of Commerce has formed the e-Commerce Policy of Pakistan (2019), wherein data protection is determined to be one of the several policy initiatives.

The above-referred laws and related rules/regulations provide for offences, enforcement and penalties related to data protection and privacy.

1.2 Regulators

The draft Bill provides for the establishment of a Commission, namely the National Commission for Personal Data Protection of Pakistan. The Commission shall be responsible for protecting the interest of individuals, to enforce protection of personal data, prevent any misuse of personal data, promote awareness of data protection and to address complaints. For the purposes of complaints, the Commission shall be deemed to be a civil court, having the same powers as are vested in a civil court under the Code of Civil Procedure, 1908.

The Commission is empowered to call for information from the data controller or from the data processor, as may be reasonably required for effective discharge of its functions. The Commission, under the draft Bill, is empowered to formulate a compliance framework regarding data audits.

As far as banking is concerned, the SBP is regulator and has the powers to call for any information related to the business of banks. The SBP has issued regulations and guidance that are to be followed by the banks; non-compliance entails penal action by the SBP.

The PTA is the regulator for the telecoms sector. It monitors and enforces the rules and regulations; non-compliance entails imposition of penalties under the PTA (Re-organization) Act, 1996.

The Federal Investigation Agency (the FIA) is the investigating agency under the PECA. The FIA and its authorised officers are empowered to investigate an offence under the PECA in accordance with the Code of Criminal Procedure, 1908.

1.3 Administration and Enforcement Process

The Commission, under the draft Bill, has the function to receive and decide complaints with regard to infringement of personal data, including violation of any provision of the draft Bill. The Commission is deemed to be a civil court for the purposes of deciding a complaint and shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908.

An individual or a relevant person may present a complaint to the Commission against a data controller or a data processer in the following matters:

- breach of a data subject's consent;
- breach of obligations of the data controller or data processer;
- providing of incomplete, misleading or false information by a data controller at the time of taking consent from a data subject; and
- any other matter related to protection or personal data.

The complaint may be filed on plain paper (or on a simplified format prescribed by the Commission). The Commission will prescribe a fee for filing and processing the complaint, and shall facilitate online receipt of complaints.

The Commission is to dispose of the complaint within 30 days of its receipt, or with reasons to be recorded in writing within such extended time as reasonably determined by the Commission.

The Commission is to afford reasonable time and opportunity to be heard to the data controller or data processer against whom a complaint is made. The Commission may also contact the complainant to seek any further information or their comments on the response of the data controller or data processer or any other concerned agency. The Commission may issue directions to stop breach of rights of a data subject without first seeking comments from the data controller or data processor.

In case of failure by the data controller or data processer to respond to the Commission or to execute its orders, the Commission may initiate enforcement proceedings.

Appeal against an order passed by any officer of the Commission lies before the Commission within 30 days of the receipt of the order. The Commission is to decide the appeal within 30 days.

Appeal against the order passed by the Commission lies before the High Court or to any tribunal established by the federal government in the manner prescribed by the High Court. The High Court or the tribunal is to decide the appeal within 90 days.

1.4 Multilateral and Subnational Issues

The draft Bill largely follows the basic principles of the GDPR. Key concepts such as "data subject", "data controller" and "data processer" have essentially similar meanings as in the GDPR. Further, the rights of the data subjects follow the same scheme. Obligations of the data controller and data processers are also mostly the same as in the GDPR.

In regard to transfer of personal data outside Pakistan, there can be seen some differences as compared to the GDPR. The draft Bill provides for cross-border transfer of personal data on account of:

- equivalent protection; and
- explicit consent of the data subject.

In the absence of an adequate data protection legal regime, the Commission may allow for the transfer of personal data in the following cases:

- binding contract/agreement;
- explicit consent of the data subject that does not conflict with the public interest or national security of Pakistan;
- international co-operation is required under relevant international obligations; and

- any further conditions specified by the Commission.

Further, critical personal data shall only be processed in a server(s) or digital infrastructure located within the territory of Pakistan. The GDPR, on the other hand, allows cross-border transfer of personal data on the basis of:

- adequate protection;
- appropriate safeguards;
- binding corporate rules;
- consent;
- necessity for the performance of a contract;
- reasons of public interest;
- necessity for the establishment, exercise or defence of legal claims; and
- necessity to protect vital interest of the data subject.

The Commission shall also devise a mechanism for sharing sensitive personal data with the government of Pakistan provided that the data relates to public order or national security, and the same data is required within the parameters of applicable law.

Another significant difference to GDPR, is the highest quantum of fine, which is 1% of the annual gross revenue in Pakistan or PKR30 million, whichever is higher. The GDPR has a maximum fine of 4% of worldwide turnover or EUR20 million, whichever is higher.

Unlawful Processing of Personal Data

Whosoever processes, disseminates or discloses any personal data in violation of the provisions of the draft Bill, shall be punished with a fine up to USD125,000, or an equivalent amount in Pakistani rupees.

Unlawful Processing of Sensitive Personal Data

Where the processing, dissemination or disclosing of sensitive personal data will be made in violation of the provisions of the draft Bill, a fine of up to USD500,000, or an equivalent amount in Pakistani rupees shall be imposed.

Unlawful Processing of Critical Personal Data

Where the processing, dissemination or disclosing of critical personal data will be made in violation of the provisions of the draft Bill, a fine up to USD1 million, or an equivalent amount in Pakistani rupees may be imposed, or as the Commission deems appropriate.

The draft Bill is a federal law applicable all over Pakistan; there are no provincial laws on this matter.

1.5 Major NGOs and Self-Regulatory Organisations

Bolo Bhi is a civil society organisation geared towards advocacy, policy and research in the areas of digital rights and civic responsibility. Bolo Bhi creates awareness of the issues related to privacy, digital safety and data protection. Bolo Bhi conducts workshops and conferences concerning privacy and data protection.

The Digital Rights Foundation is a research-oriented, not-for-profit organisation focusing on information and communication technology to support human rights, democratic processes and digital governance. The Digital Rights Foundation seeks to increase awareness of privacy issues and defend the right to privacy by research.

Both the above organisations have submitted their comments on the draft Bill to the Ministry.

1.6 System Characteristics

The draft Bill would override other laws. However, in case any other law provides for more stringent provisions regarding the subject matter, then the more stringent provisions will prevail.

The draft Bill does not follow a sectoral approach and is equally applicable to all commercial, non-commercial, economic and industrial sectors.

The draft Bill has a "right-based" approach whereby extensive rights are conferred on the data subjects and, conversely, obligations are imposed on the data controllers and data processers. In essence, the draft Bill aims to protect the privacy rights of individuals.

1.7 Key Developments

In April 2021, a Constitutional Petition was filed before the Sindh High Court (High Court in the province of Sindh) seeking issuance of a direction to the federal government to promulgate necessary laws for the protection of the mobile phone data of citizens. The Ministry submitted before the Court that the draft bill of personal data protection was ready and under a consultation process. The petitioner had approached the Court on the grounds of media reports highlighting that personal data of mobile phone users had been breached. The petition has not been finally decided yet, but the petition is likely to further expedite the law-making process on the subject.

In July 2021, the government of Pakistan framed its National Cyber Security Policy 2021. A Cyber Governance Policy Committee (CGPC) has been constituted for strategic oversight over national cybersecurity issues. One of the functions of the CGPC is to formulate the Cyber Security Act.

In October 2021, the PTA issued Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2021. These rules provide powers to the PTA for removal of online content, filing of complaints and implementing oversight mechanisms in relation to online content. The PTA may remove or block online content if this is in the interest of:

- the glory of Islam;
- the security of Pakistan;
- public order;
- decency or morality; or
- the integrity or defence of Pakistan.

1.8 Significant Pending Changes, Hot Topics and Issues

It is expected that the draft Bill will be promulgated as a law. The Ministry may also commence the development of Cyber Security Act as per the National Cyber Security Policy 2021.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

The draft Bill is applicable to:

- any data controller or a data processor, who processes or has control over or authorises the processing, where the data controller or data processer is established or located in Pakistan;
- the data controller or data processer who is digitally or non-digitally operational in Pakistan (but incorporated outside Pakistan) and is involved in commercial or non-commercial activity (including profiling data subjects) in Pakistan;
- processing of personal data by a data controller or data processer who is not established in Pakistan, but in a place where

Pakistani law applies by virtue of private and public international law; and
- any data subject (including a foreign data subject) present in Pakistan, provided that, in case of foreign data subject, the collection is not in conflict with the privacy laws of the country where the data controller is registered.

The Data controller/data processor identified as "significant" by the Commission shall be required to appoint a data protection officer, who is well-versed in the collection and processing of personal data and the risks associated with the processing. Moreover, the draft Bill empowers the Commission to formulate a compliance framework regarding the responsibilities of a data protection officer. Once the Commission is established, it is likely that it will devise a mechanism for the appointment and responsibilities of the data protection officer.

General principles or criteria necessary to authorise to collect, use and process personal data are:

- a lawful purpose directly related to an activity of the data controller;
- such processing is necessary for, or directly related to, the lawful purpose;
- the personal data collected is adequate but not excessive in relation to the lawful purpose; or
- there is consent by the data subject.

The following are exceptions to the requirement of consent by the data subject:

- performance of a contract to which the data subject is a party;
- taking steps at the request of the data subject to enter into a contract;
- for treatment, public health, medical or research purposes or to respond to any medical emergency involving a threat to the life or the health of a data subject or any other individual;
- compliance with any legal obligation to which the data controller is the subject (other than contractual obligation);
- to protect the vital interests of the data subject;
- for the administration of justice pursuant to an order of the court of competent jurisdiction;
- for legitimate interests pursued by the data controller; or
- for exercise of any functions conferred on any person by or under any law.

The data controller is required to give a written notice to the data subject informing them of the following:

- that their personal data is being collected, together with a description of the personal data so collected;
- the legal basis for the processing of the personal data;
- the duration for which data is to be processed;
- the time period for which personal data is likely to be retained;
- the purpose for which personal data is being collected and further processed;
- information, available from the data controller, as to the source of the personal data;
- the data subject's rights;
- the data subject's right to access and request correction, and a description of how to contact the data controller for any inquiries or complaints;
- the class of third parties to whom the data subject discloses or may disclose the personal data;

- the choices and means offered by the data controller for restricting the processing of personal data;
- whether it is obligatory or voluntary for the data subject to supply personal data; and
- where it is obligatory for the data subject to supply the personal data, the consequences if the data subject fails to supply their data.

This written notice is to be given as soon as reasonably possible, namely:

- when the data subject is first asked by the data controller to provide personal data;
- when the data controller first collects the personal data;
- before the data controller uses the personal data of the data subject for a purpose other than that for which it was collected; and
- before the data controller discloses the personal data to a third party.

The draft Bill does not contain the concepts of "privacy by design" or "privacy by default". The Commission, based upon national interest, is to prescribe best international standards to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. The data controller and data processer are to follow the standards so prescribed by the Commission. The standards to be prescribed by the Commission may account for the concept of "privacy by design" or "privacy by default".

The draft Bill requires that the data controller is to take adequate steps to ensure that personal data is accurate, complete, not misleading and is kept up to date with regard to the purpose for which it is collected and further processed.

The data controller is to keep and maintain record of each application, notice, request or any other information relating to personal data that has been or is being processed by the data controller. The Commission is to determine the manner and form in which such record is to be maintained.

The draft Bill does not contain any specific provision with regard to conducting privacy, fairness or legitimate impact analysis. Likewise, there is no specified requirement regarding adoption of internal or external privacy policies. The draft Bill empowers the Commission to formulate a compliance framework regarding data protection impact assessment and privacy. Once the Commission is established, it is likely it will devise mechanisms for data protection impact assessment and adoption of privacy policies.

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

- right to access;
- right to correct;
- right to withdraw consent;
- right to prevent processing;
- right to erasure;
- right to nominate;
- right to redressal of grievance; and
- right to data portability.

Anonymised Data

According to the law, anonymised data means personal data which has undergone the irreversible process of transforming or converting personal data to a form in which a data subject cannot be identified.

Pseudonymised Data

The draft Bill does not define pseudonymised data, however it refer pseudonymisation as 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 is not attributed to an identified or identifiable natural person.

The draft Bill provides that a data subject has the right not to be subjected to a decision solely based on automated processing, including profiling. As a consequence, it follows that profiling, online monitoring or tracking based upon big data analysis, artificial intelligence or by use of algorithms are not permitted.

The draft Bill provides for imposition of monetary penalties. However, there is no concept of compensation to an aggrieved person arising out of the breach of personal data.

2.2 Sectoral and Special Issues

Sensitive personal data, under the draft Bill, means data relating to access control, financial information excluding identification number (bank account, credit/debit card, account number, or other payment instruments data) computerised national identity card, passport, biometric data, health data (physical, behavioural, psychological and mental health conditions, or medical records), medical records, ethnicity, religious beliefs, criminal records, genetic data, political affiliation, physical identifiable location, travelling details, pictorial or graphical still and motion forms, IP address and online identifier.

Sensitive personal data may only be processed under the following situations:

- with the explicit consent of the data subject (when that consent is not restricted by any other applicable law);
- for the purposes of exercising or performing any right or obligation imposed by law on the data controller in connection with employment;
- to protect the vital interests of the data subject;
- for medical purposes;
- in connection with any legal proceedings;
- for obtaining legal advice (while ensuring its integrity and secrecy);
- for the purposes of establishing, exercising or defending legal rights;
- processing is necessary for the administration of justice pursuant to orders of a court of competent jurisdiction; or
- for the exercise of any functions conferred on any person by or under any law.

Physical identifiable location, IP address and online identifier are included within the definition of "sensitive personal data". Therefore, browsing data, viewing data, cookies, beacons and location data (pertaining to IP address and physical identifiable location) are subject to the same rules, as "sensitive personal data".

Communications data, voice telephony and text messaging, content of electronic communications, children's or students' data and employment data are not covered under the definition of "sensitive personal data" and, therefore, general principles (or criteria) – as explained at **2.1 Omnibus Laws and General Requirements** – are applicable to this class of data.

While laying down the conditions for children's personal data processing, the draft Bill states that a data controller or a data processor shall not undertake tracking or behavioural monitor-

ing of children or targeted advertising directed at children.

The conduct of social media or social network service is governed under the Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2021, as discussed at **1.7 Key Developments**.

The financial sector (banks, etc) is governed by the SBP. The following regulations are required for security of customers' information:

- SBP Regulations for the Security of Internet Banking;
- SBP Regulations for Payment Card Security;
- SBP Regulations for Electronic Money Institutions; and
- SBP (Payment System Department) Circular No 9 of 2018, dated 28 November 2018.

The Credit Bureaus Act regulates the obligations of credit bureaus as to fidelity, confidentiality and secrecy.

The Electronic Funds Transfer Act also requires that a financial institution shall not divulge any information relating to an electronic fund transfer or the account of its customers, except as required by law.

PTA has issued various regulations encompassing consumer protection, including in regard to consumers' personal information. The following regulations are relevant:

- Telecom Consumers Protection Regulations, 2009;
- Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations, 2009;
- Subscribers Antecedents Verification Regulations, 2015;
- Regulations for Technical Implementation of Mobile Banking, 2016;
- Data Retention of Internet Extended to Public Wi-Fi Hotspots Regulations, 2018; and
- Critical Telecom Data and Infrastructure Security Regulations, 2020.

The following are recognised as offences under the PECA:

- unauthorised access to information system or data;
- cyberterrorism;
- hate speech;
- electronic forgery;
- electronic fraud;
- unauthorised use of identity information;
- offences against the dignity of a natural person;
- offences against the modesty of a natural person and minor;
- child pornography; and
- spamming.

2.3 Online Marketing

Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations, 2009 requires all operators (holding a licence from the PTA) to establish a standard operating procedure (duly approved by the PTA) to control spamming.

Similarly, all 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.

The draft Bill does not contain any provision with respect to behavioural and targeted advertising.

2.4 Workplace Privacy

Pakistan has no specific law concerning workplace privacy. The draft Bill provides that sensitive personal data may be processed by a data controller for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

The Public Interest Disclosures Act, 2017 governs the mechanism for public interest disclosures and protection of persons making such disclosures (related to the prevention of corruption in public sector organisations). Anonymous or pseudonymous disclosures are not entertained under this Act. The identity of the complainant is to be protected unless required otherwise. The Act provides protection to the complainant against any victimisation on the ground that they made a disclosure. A complainant is considered victimised if they are:

- dismissed;
- suspended;
- denied promotion;
- demoted;
- made redundant;
- harassed;
- intimated;
- threatened with any of the above matters; or
- subjected to a discriminatory or other adverse measures by their employer or by a fellow employee.

This Act also provides for due protection of the complainant, witness or any other person rendering assistance for an inquiry.

The Securities and Exchange Commission of Pakistan (SECP) has issued Listed Companies (Code of Corporate Governance) Regulations, 2019 (the "Code"). The Code requires that listed companies' board of directors maintain a whistle-blowing policy, by establishing a mechanism to receive and handle complaints in a fair and transparent manner while providing protection to the complainant against victimisation. The Code requires that the chief executive officer of a listed company place "reports on/synopsis of issues and information pursued under the whistle-blowing policy, clearly disclosing how such matters were dealt with and finally resolved or cancelled", before the board of directors or before the committee of the board of directors.

Matters pertaining to the role of labour organisations, e-discovery issues, use of digital loss prevention technologies and scanning/blocking websites at a workplace are not dealt with under the draft Bill or under any other law.

2.5 Enforcement and Litigation

The Commission, under the draft Bill, is empowered to formulate a compliance framework regarding a grievance redressal mechanism. The Commission would have powers of search and seizure while dealing with complaints. The detailed procedural aspects will be devised upon establishment of the Commission. However, considering the established legal norms in Pakistan, the detailed procedure is likely to ensure the following core principles:

- opportunity of being heard;
- fair trial; and
- due process.

The draft Bill provides for the following financial penalties:

- a fine of up to USD125,000 or an equivalent amount in Pakistani rupees, in case of processing of personal data in violation of any provision of the draft Bill (which may be raised to USD250,000 or an equivalent amount in Pakistani rupees, in case of subsequent unlawful processing);
- a fine of up to USD500,000 or an equivalent amount in Pakistani rupees, in case of processing of sensitive personal data in violation of any provision of the draft Bill;
- a fine of up to USD1 million or an equivalent amount in Pakistani rupees or as the Commission deems appropriate in case of processing of critical personal data in violation of any provision of the draft Bill;
- a fine of up to USD50,000 or an equivalent amount in Pakistani rupees, on failure to adopt security measures required under the draft Bill;
- a fine of up to USD50,000 or an equivalent amount in Pakistani rupees, on failure to comply with the orders of the Commission or of the court;
- a fine of up to USD2 million or an equivalent amount in Pakistani rupees, when any person fails to respond to an enforcement notice issued by the Commission, or fails to satisfy the Commission about an alleged contravention, or fails to remedy the contravention within the time allowed by the Commission; and
- a fine of up to 1% of annual gross revenue in Pakistan or USD200,000, whichever is higher, or an equivalent amount in Pakistani rupees, in case of a legal person.

In view of the fact that there is no law on the protection of personal data, there are no enforcement cases to be mentioned here.

A private litigation, for alleged privacy or data protection violations, would be subjected to basic legal norms as mentioned above (ie, opportunity of being heard, fair trial and due process).

Class actions are only allowed under certain specific laws – for instance, by creditors in case of a winding-up petition under the Companies Act, 2017. Trade and consumer associations may also bring class actions in the matters of competition, consumer protection and anti-dumping investigations.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

The Investigation for Fair Trial Act, 2013 (the "Fair Trial Act") provides for the matters related to surveillance and interception in relation to investigation of offences specified in the Schedule I to the Fair Trial Act. The offences pertain to the following laws:

- the Private Military Organizations Abolition and Prohibition Act, 1974;
- the Prevention of Anti-National Activities Act, 1974;
- the Anti-Terrorism Act, 1997;
- the Pakistan Nuclear Regulatory Authority Ordinance, 2001; and
- the National Command Authority Act, 2010.

The official of the applicant (the department seeking permission for surveillance or interception) is first to seek permission of the federal Minister of the Interior through its head of department.

After receiving permission from the Minister of the Interior, the authorised officer of the appli-

cant department makes an application to the judge of the High Court for issuance of a warrant for surveillance or interception. Only if the judge passes an order for the issuance of a warrant may the applicant proceed to surveillance or interception.

In regard to protection of privacy, the Fair Trial Act has the following provisions:

- the application for issuance of a warrant is to be accompanied by a signed statement and affidavit to the effect that approval of the warrant shall not be abused to interfere or intervene in the privacy of any person;
- the judge, while passing the order for issuance of a warrant, is to consider that issuance of a warrant shall not unduly interfere in the privacy of any person or property;
- where the judge is of the view that any request for issuance of warrant has resulted in undue and inappropriate interference in the privacy of any person, then they may recommend departmental action against the concerned officer;
- the judge is to ensure that, under the Fair Trial Act, no disclosure of any source of information is made that may compromise the future capability of the applicant department's intelligence gathering; and
- the material intercepted pursuant to the warrant shall only be used in accordance with the Fair Trial Act.

Any person carrying out surveillance or interception, except in accordance with the Fair Trial Act, is to be punished with imprisonment up to three years (in addition to any other punishment under any other law).

3.2 Laws and Standards for Access to Data for National Security Purposes

Laws and standards for access to data for intelligence, anti-terrorism or other national security purposes are as discussed at **3.1 Laws and Standards for Access to Data for Serious Crimes**.

3.3 Invoking Foreign Government Obligations

The draft Bill does not recognise a foreign government access request as a legitimate basis to transfer personal data outside Pakistan.

Pakistan does not participate in a Clarifying Lawful Overseas Use of Data (CLOUD) Act agreement with the USA.

3.4 Key Privacy Issues, Conflicts and Public Debates

The draft Bill is facing criticism in relation to the following matters:

- restriction of cross-border transfer of personal data;
- data localisation requirement;
- certain relaxations available to government departments; and
- rule-making (security standard setting) powers of the Commission – critics hold the view that security standards should be part of the substantive legislature and not left for subordinate legislation by the executive.

4. International Considerations

4.1 Restrictions on International Data Issues

Transfer of personal data outside Pakistan, under the draft Bill, is only permissible in the following cases:

- equivalent protection;
- explicit consent of the data subject; and
- under a framework to be devised by the Commission.

In the absence of an adequate data protection legal regime, the Commission may allow for the transfer of personal data outside Pakistan in the following cases:

- binding contract/agreement;
- explicit consent of the data subject that does not conflict with the public interest or national security of Pakistan;
- international co-operation is required under relevant international obligations; and
- any further conditions specified by the Commission.

It should be noted that critical personal data is not allowed to be transferred outside Pakistan.

The Commission, under the draft Bill, is required to devise a mechanism for keeping some components of sensitive personal data within Pakistan (ie, data localisation).

The Commission shall also devise a mechanism for sharing sensitive personal data with the government of Pakistan provided that the data relates to public order or national security and the same is required within the parameters of applicable law.

4.2 Mechanisms or Derogations That Apply to International Data Transfers

With respect to international data transfer, the draft Bill only provides the mechanism as discussed in **4.1 Restrictions on International Data Issues**.

4.3 Government Notifications and Approvals

Under the draft Bill, one of the permissible modes of cross-border transfer of personal data is a "mechanism to be devised by the Commission". On establishment of the Commission, the mechanism may contain any approval requirements for all or any class of personal data.

4.4 Data Localisation Requirements

The draft Bill provides that the Commission is to devise a mechanism for keeping some components of sensitive personal data in Pakistan. Conversely, critical personal data is only to be processed in a server or data centre located in Pakistan. The projected data localisation mechanism will be known once framed by the Commission after its establishment; as a corollary, it follows that sensitive personal data may be transferred outside Pakistan with the requirement to keep some component in Pakistan.

4.5 Sharing Technical Details

There are no statutory requirements to share any software code, algorithms or similar technical details with the government.

4.6 Limitations and Considerations

The only limitations and considerations regarding international transfer of personal data are those discussed at **4.1 Restrictions on International Data Issues**. The draft Bill does not contain any provision in relation to foreign government data requests, foreign litigation proceedings or internal investigations.

4.7 "Blocking" Statutes

There are no blocking statutes, related to data privacy or otherwise.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

The government's Digital Pakistan Policy sets the goals and directions for IoT, fintech, artificial intelligence and robotics, cloud computing and big data. However, there is no law or regulation at present.

The SECP has issued draft Cloud Adoption Guidelines for Incorporated Companies/Business Entities (BEs). The draft Guidelines treat "personally identifiable information" (PII) as sensitive official data. As per the draft Guidelines, the PII is any data that could potentially be used to identify a particular person. The draft Guidelines require that, in case of PII, only the most secure cloud service providers should be relied upon; the Guidelines further require that BEs need to encrypt PII and ensure that the key and encrypted PII is not stored on the same cloud.

The draft Bill provides a data subject the right not to be subject to a decision based solely on automated processing, including profiling.

Biometric data and physical identifiable location (ie, geolocation) are included within the definition of "sensitive personal data", and hence provisions of the draft Bill are applicable on biometric and physical identifiable location, as explained at **2.2 Sectoral and Special Issues**.

Matters related to disinformation, deepfakes, online harms, dark pattern or online manipulation are dealt with under the Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2021, as discussed at **1.7 Key Developments**.

The Civil Unmanned Aircraft System Act, 2021 has been tabled before the National Assembly of Pakistan, but has not yet been passed. This Act intends to establish the Civil Unmanned Aircraft System Authority. Once established, this Authority will be responsible for the regulation and control of civil unmanned aircraft systems (ie, drones).

5.2 "Digital Governance" or Fair Data Practice Review Boards

Currently, there is no practice concerning digital governance or fair data practice. Once the draft Bill becomes law, such practices may emerge as the precise legalities of this subject matter evolve.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

Currently, there is no law in Pakistan regarding protection of personal data, so there are no issues regarding enforceability, penalties or related litigation.

5.4 Due Diligence

There is no uniform or statutory process concerning due diligence in corporate transactions. The entities perform due diligence based upon their individual risk appetite and underlying circumstances, with regard to the nature and complexity of a particular transaction.

5.5 Public Disclosure

Currently, there is no requirement for making public disclosure regarding an organisation's cybersecurity risk profile or experience.

5.6 Digital Technology Regulation/ Convergence of Privacy, Competition and Consumer Protection Laws (Including AI)

Pakistan has launched the Public Key Infrastructure (PKI) for the National Root Certification Authority. PKI governs the issuance of digital certificates to protect data, provide unique digital identities for users, devices and applications and secure end-to-end communications. The PKI will tend to establish trust and security in electronic transactions which will augment e-commerce in the country.

5.7 Other Significant Issues

In July 2021, the government of Pakistan framed its National Cyber Security Policy. To achieve the objectives of this Policy, an implementation framework shall be developed by a designated organisation of the federal government.

The implementation framework will set out the government's vision to manage and implement cybersecurity practices at a national level. The framework will consist of the following areas:

- active defence;
- protecting internet-based services;
- protection and resilience of the national critical information infrastructure;
- protection of the government's information systems and infrastructure;
- information security assurance framework;
- public-private partnership;
- cybersecurity research and development;
- capacity building;
- awareness for a national culture of cybersecurity;
- global co-operation and collaboration;
- cybercrime response mechanism; and
- regulations.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com