COUNTRY COMPARATIVE GUIDES 2022

The Legal 500 Country Comparative Guides

Pakistan

DATA PROTECTION & CYBER SECURITY LAW

Contributing firm

S.U.Khan Associates Corporate & Legal Consultants

Saifullah Khan

Managing Partner | saifullah.khan@sukhan.com.pk

Saeed Hasan Khan

Partner | saeed.hasan@sukhan.com.pk

This country-specific Q&A provides an overview of data protection & cyber security law laws and regulations applicable in Pakistan.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

PAKISTAN
DATA PROTECTION & CYBER SECURITY LAW

1. Please provide an overview of the legal and regulatory framework governing data protection and privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the relevant laws). Are there any expected changes in the data protection and privacy law landscape in 2022-2023 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

Privacy is a fundamental and inalienable right under the Constitution of Pakistan. Pakistan is in the process to develop a specific law on personal data protection. A draft bill (Personal Data Protection Act, 2021/"the draft Bill") has been developed by the Ministry of Information Technology and Telecommunication. The draft Bill has been approved by the Federal Cabinet and will now be presented before the legislature (National Assembly and Senate of Pakistan) and thereafter will be promulgated as a law. The draft Bill is not sector-specific but is applicable on processing of personal data by any sector. The draft Bill is applicable when either of data controller, data processer or data subject is present in Pakistan. The draft Bill would also be applicable to those data controllers and data processers who are not incorporated in Pakistan but are digitally or non-digitally operational in Pakistan and are involved in commercial or non-commercial activity in Pakistan. The draft Bill would also be applicable on processing of personal data by data controllers and data processers who are not established in Pakistan but are in a place where Pakistan law is applicable due to private or public international law.

On promulgation of the draft Bill as a law, a National Commission for Personal Data Protection of Pakistan (the Commission) is to be established by the Federal Government of Pakistan. The Commission will be a regulator and will enforce and implement the draft Bill.

Apart from above, sectoral regulatory framework concerning data protection may be seen for banking and telecom sectors. State Bank of Pakistan (the SBP) and Pakistan Telecommunication Authority (the PTA) respectively are the regulators for banking and telecom sectors in Pakistan. The SBP and the PTA have developed certain regulations concerning the protection of their respective consumers including regulations for protection of personal data of the banking and telecom consumers.

2. Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?

The draft Bill does not place any specific requirement for registration or licensing of data controllers or data processers. The draft Bill, however, while describing the functions of the Commission provides that the Commission is to formulate a registration framework for data controllers and data processers. It follows that the Commission after its establishment may formulate registration regime for the data controllers and data processers.

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

"**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 and/or data processor, including any sensitive personal data. Provided that anonymized, or pseudonymized data which is incapable of identifying an individual is not

personal data.

"**sensitive personal data**" means and includes data relating to access control (username and/or password), financial information such as bank account, credit card, debit card, or other payment instruments, computerized national identity card, passports, biometric data, and physical, behavioral, psychological, and mental health conditions, medical records, and any detail pertaining to an individual's ethnicity, religious beliefs, political affiliation, physical identifiable location, travelling details, pictorial or graphical still and motion forms, IP address and online identifier.

"**critical personal data**" means and includes data relating to public service providers, unregulated e-commerce transactions and any data related to international obligations.

"**data subject**" means a natural person who is the subject of the personal data.

"**data controller**" means a natural or legal person or the government, who either alone or jointly has the authority to make a decision on the collection, obtaining, usage or disclosure of personal data.

"**data processor**" means a natural or legal person or the government who alone or in conjunction with other(s) processes data on behalf of the data controller.

"**processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**consent**" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the collecting, obtaining and processing of personal data relating to him or her.

"**personal data breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

4. What are the principles related to, the general processing of personal data or PII – for example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction or must personal data or PII only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

The draft Bill provides following general principles for processing of personal data:

- Personal data be collected for specified, explicit and legitimate purpose
- Personal data is not to be processed in a manner incompatible with the purposes for which it was collected
- Personal data is to be adequate, relevant and limited to what is necessary in relation to the purpose for which it was collected
- Personal data is to be processed for a lawful purpose directly related to an activity of the data controller
- Processing of personal data is necessary or is directly related to that lawful purpose
- Personal data is adequate and not excessive in relation to that lawful purpose

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

As a general rule no personal data is to be processed without consent of the data subject. A separate consent is required form data subject for each purpose. The draft Bill provides following exceptions when personal data may be processed without consent of the data subject:

- When processing is necessary for the performance of a contract to which the data subject is a party
- When processing is necessary for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by a contract
- When processing is necessary to protect the vital interests of the data subject
- When processing is necessary for the administration of justice pursuant to an order of the court of competent jurisdiction
- When processing is necessary for legitimate interests pursued by the data controller
- When processing is necessary for the exercise of any functions conferred on any person by

or under any law

6. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

The draft Bill does not speak about the form, content and administration of the consent. The definition of "consent" as provided for in the draft Bill depicts the underlying concept based upon the principles of freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the collecting, obtaining and processing of personal data relating to him or her. So the form may not be as important but the substance should be met.

7. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

Under the draft Bill, sensitive personal data may only be processed in 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
- for the exercise of any functions conferred on any person by or under any law

There are no categories of personal data which are prohibited from collection under the draft Bill.

8. How do the laws in your jurisdiction address children's personal data or PII?

The draft Bill does not address processing of children's personal data.

9. Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

The draft Bill is not applicable on an individual processing personal data only for the purposes of his personal, family, household and recreational purposes.

10. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

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".

11. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

The data controllers are to intimate the Commission on a regular basis the type of data they are collecting and processing. Procedural aspects for this reporting requirements are to be devised by the Commission.

In addition, 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. As the law, on the subject, has not been promulgated yet therefore practically such requirements are not being met.

12. Do the laws in your jurisdiction require or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

The draft Bill provides that personal data processed shall not be kept longer than is necessary for the fulfillment of the purpose or as required under the law. The draft Bill further mandates the data controller to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.

13. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

The draft Bill does not place any mandatory requirement on the data controllers or the data subjects to consult with the Commission. However, one of the functions of the Commission under the draft Bill is to engage, support, guide, facilitate, train and persuade data controllers and data processers to ensure personal data protection. It follows that the Commission may contact data controllers/data processors in furtherance of the objects of the draft Bill.

14. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

The draft Bill does not require or recommend conducting risk assessment regarding personal data processing activities. However, the draft Bill empowers the Commission to formulate a compliance framework with regard to data protection impact assessment. It follows, that on promulgation of law and after establishment of the Commission, the Commission will frame rules with respect to data protection impact assessment.

15. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?

The draft Bill does not require to appoint a data protection officer. However, the draft Bill empowers the Commission to formulate a compliance framework with regard to responsibilities of data protection officer. It follows, that on promulgation of law and after establishment of the Commission, the Commission will frame rules with respect to appointment of data protection officer.

16. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

The draft law does not require or recommend employee training.

17. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (e.g., posting an online privacy notice).

The draft Bill provides that a data controller is to give a written notice to the data subject. The said notice is to inform the data subject following:

- That personal data of the data subject is being collected and a description of the personal data
- The legal basis for processing of personal data
- The time duration for which personal data is likely to be processed and retained
- The purpose for which personal data is being collected and further processed
- The information as to source of the personal data
- The data subject’s right to request access the data and to request correction and how to contact the data controller for any inquiries or complaints
- The class of third parties to whom data is disclosed or to be disclosed
- The choices and means data controller offer for restricting processing of personal data
- Whether it is obligatory or voluntary for the data subject to provide personal data and

where it is obligatory the consequences for failure to provide personal data

The said notice is to be given as soon as reasonably possible when:

- The data subject is first asked by the data controller to provide personal data
- The data controller first collects the personal data
- Before the data controller uses personal data for a purpose other than the purpose for which personal data was collected
- Before the data controller discloses the personal data to a third party

The said notice is to be given in Urdu and English languages with clear and readily accessible means to exercise choice by the data subject.

18. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (e.g., are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

The draft Bill distinguishes between the data controller and data processer (as defined at question 3). The data controller is to ensure that data processer undertakes to adopt applicable technical and organizational security standards to protect the personal data. The draft Bill further requires that the data processer is independently liable to take steps to ensure compliance with the prescribed security standards.

19. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

The draft Bill does not provide any guidance on contractual arrangements between the data controllers and the data processers.

20. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions are imposed, if any?

The draft Bill provides a right to the data subjects to not to be subjected to a decision solely based on automated processing including profiling. These terms have not been defined in the draft Bill. No further details/restrictions are mentioned in the draft Bill.

21. Please describe any restrictions on cross-contextual behavioral advertising. How is this term or related terms defined?

The draft Bill does not discuss about cross-contextual behavioral advertising, except the right to the data subjects against the automated decision making and profiling.

22. Please describe any laws in your jurisdiction addressing the sale of personal information. How is "sale" or related terms defined and what restrictions are imposed, if any?

The sale of personal information is not currently addressed in any law.

23. Please describe any laws in your jurisdiction addressing telephone calls, text messaging, email communication or direct marketing. How are these terms defined and what restrictions are imposed, if any?

The Pakistan Telecommunication Authority (the PTA) has issued "Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations, 2009" (the Regulations). The Regulations apply to all telecom operators licensed by the PTA to ensure and protect the interests of telecom consumers by preventing them from spam, fraudulent, unsolicited and obnoxious communication. A few important terms are defined by the Regulations as follows:

"**Do Not Call Register (DNCR)**" means a database, maintained by the operators, containing the particulars of subscriber(s) who make a request for not receiving the unsolicited calls.

"**Fraudulent Communication**" means the transmission

of message/statement which is false and misleading.

"**Obnoxious Communication**" means the transmission of message/statement with the intent to cause harassment or disturbance.

"**Spamming**" means the transmission of harmful, fraudulent, misleading, illegal or unsolicited messages in bulk to any person without the express permission of the recipient, or causing any electronic system to show any such message or is being involved in falsified online user account registration or falsified domain name registration for commercial purpose.

"**Telemarketer**" means a person who initiates a call for the purpose of marketing of services, investment and goods to public at large through telecommunications services.

"**Unsolicited calls**" means calls made to those numbers recorded in the Do not call register.

The Regulations require all operators to establish standard operating procedures to control spamming, fraudulent communication, unsolicited calls and obnoxious calls. The operators are also required to establish a "Do Not Call Register" in connection with controlling unsolicited calls. The Operators are also required to ensure registration of telemarketers.

24. Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these terms defined and what restrictions are imposed, if any?

Biometric is included within the definition of "sensitive personal data" and rules as explained at question 7 are applicable in relation thereto.

25. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

The draft Bill provides that personal data may be transferred outside Pakistan in following situations:

- Equivalent protection
- Consent of the data subject
- Under a framework to be devised by the Commission

Critical personal data is not allowed to be transferred outside Pakistan. The Commission is to devise a mechanism for keeping some components of sensitive personal data within Pakistan (data localization of some of the sensitive personal data).

26. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

The Commission, considering the national interest, is to prescribe best international standards to protect personal data from any loss, misuse, modification, unauthorized or accidental access, disclosure, alteration or destruction. Data controllers and data processers are to take practical measures, while processing personal data, as prescribe by the Commission to protect the personal data.

27. Do the laws in your jurisdiction address security breaches and, if so, how does the law define "security breach"?

The term "personal data breach" is defined in the draft Bill as mentioned at question 3.

28. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

The draft Bill does not provide any sector specific security requirements.

29. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

The draft Bill requires the data controller to report a data breach to the Commission and to the data subject within 72 hours. The exception is where the personal data breach is unlikely to result in a risk to the rights and

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

The notification must contain the following information:

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

30. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

The Prevention of Electronic Crimes Act, 2016 (the PECA) was promulgated to prevent unauthorized acts with respect to information systems and to provide for related offences and mechanism for their investigation, prosecution and trial. The PECA is a criminal law and recognizes various acts as being an offence like:

- Unauthorized access to information system or data
- Unauthorized copying or transmission of data
- Interference with information system or data
- Electronic forgery
- Electronic fraud
- Unauthorized use of identity information

31. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

Pakistan has no separate cybersecurity regulator. The Federal Investigations Authority is responsible to implement and enforce the PECA with reference to cyber-crimes.

32. Do the laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

The draft Bill confers following rights to the data subjects, exercisable through submission of a request to data controller:

- Right of access to personal data
- Right to correct personal data
- Right to withdrawal of consent
- Right to prevent processing likely to cause damage or distress
- Right to erasure
- Right to data portability
- Right not to be subjected to a decision solely based on automated processing including profiling

The draft Bill provides the instances where a data controller may refuse to comply with a request by data subject to have these rights, as follows:

Right of Access to Personal Data

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

Right to Correct Personal Data

- The data controller is not supplied with such information as the data controller may reasonably require.
- The data controller is not supplied with such

information as it may reasonably require to ascertain in what way the personal data to which the data correction request relates is inaccurate, incomplete, misleading or not up-to-date.
- The data controller is not satisfied that the personal data to which the data correction request relates is inaccurate, incomplete, misleading or not up-to-date.
- The data controller is not satisfied that the correction which is the subject of the data correction request is accurate, complete, not misleading or up-to-date.
- Where any other data controller controls the processing of the personal data to which the data correction request relates in such a way as to prohibit the first-mentioned data controller from complying, whether in whole or in part, with the data correction request.

Right to Prevent Processing Likely to Cause Damage or Distress

- Where the data subject has given his consent.
- Where the processing of personal data is necessary:
- for the performance of a contract to which the data subject is a party.
- for the taking of steps at the request of the data subject with a view to entering a contract.
- for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by contract.
- in order to protect the vital interests of the data subject.

Right to Erasure

When processing is necessary for:

- Exercising the right of freedom of expression and information.
- Compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Reasons of public interest in the area of public health.
- Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- The establishment, exercise or defence of legal claims.

33. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

To enforce the individual data privacy rights a data subject is to present a complaint before the Commission. In case the data subject is not satisfied with the decision in complaint (of the Commission), the data subject has the right to present an appeal before the High Court or to the Tribunal established by the Federal Government for the purpose in the manner prescribed by the High Court.

34. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

An individual or relevant person, under the draft Bill, may file a complaint on its own before the Commission against any violation of personal data protection rights conferred under the draft Bill, conduct of any data controller, data processer or their processes

35. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

The draft Bill does not provide for entitlement for any monetary damages or compensation to the affected data subjects.

36. How are the laws governing privacy and data protection enforced?

The Commission would act as a regulator and enforcer of the subject matter. The data subjects may file a complaint to the Commission for enforcement of their rights, as explained at question 34.

37. What is the range of sanctions (including fines and penalties) for violation of these laws?

Offence	Fine
A data controller not ceasing the processing of personal data after withdrawal of consent by the data subject.	Fine of up to PKR 5 million (US$ 27,300 approx.).
Anyone who processes or cause to be processed, disseminates or discloses personal data in violation of the draft Bill.	Fine of up to PKR 15 million (US$ 81,900 approx.) and in case of a subsequent unlawful processing the fine may be raised up to PKR 25 million (US$ 136,600 approx.). In case of sensitive personal data the fine is up to PKR 25 million (US$ 136,600 approx.).
Failure to adopt the security measures that are necessary to ensure data security.	Fine of up to PKR 5 million (US$ 27,300 approx.).
Failure to comply with the orders of the National or the court.	Fine of up to PKR 2.5 million (US$ 13,600 approx.).
Failure to comply with the directions of the Commission.	Fine of up to PKR 250 million (US$ 1,366,000 approx.).
Corporate liability.	Fine of up to PKR 30 million (US$ 163,900 approx.) or 1% of annual gross revenue, whichever is higher.

38. Are there any guidelines or rules published regarding the calculation of fines or thresholds for the imposition of sanctions?

The draft Bill does not provide any guidelines or rules regarding the calculation of fines or thresholds for imposition of sanctions.

39. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

Orders of the Commission are appealable to the High Court (or to a Tribunal established by the Federal Government for the purpose in the manner prescribed by the High Court). Any person aggrieved by the order of the Commission may prefer such an appeal.

40. Are there any proposals for reforming data protection or cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

The foremost is to present the draft Bill before the legislature for promulgating as a law. Apart from this, in July 2021 the Government of Pakistan has framed its National Cybersecurity Policy. Based upon this Policy, Cyber Security Act is to be formulated. It is expected that soon the work on development of Cyber Security Act will commence.

Contributors

Saifullah Khan
Managing Partner
saifullah.khan@sukhan.com.pk

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