DigitalRightsFoundation

"KNOW YOUR RIGHTS"

DATA PRIVACY BOOKLET FOR

JUDICIARY

Table of Contents

About Us

Digital Rights Foundation (DRF) is a registered research-based advocacy non-governmental organization in Pakistan. Founded in 2012, DRF focuses on ICTs to support human rights, inclusiveness, democratic processes, and digital governance. DRF works on issues of online free speech, privacy, data protection and online violence against women. DRF opposes any and all sorts of online censorship and violations of human rights both on-ground and online.

For more information visit:
www.digitalrightsfoundation.pk

Acknowledgements

This literature has been authored by Zainab Durrani, Anam Baloch and Minahil Farooq and has been edited by Seerat Khan. The design is credited to Ahsan Zahid and Talha Umar.

Disclaimer

Every effort has been made to ensure the accuracy of the contents of this publication. The authors or the organization do not accept any responsibility of any omission as it is not deliberate. Nevertheless, we will appreciate the provision of accurate information to improve our work.

Aims and objectives

Through this booklet we aim to provide resources and literature to the judiciary of Pakistan and facilitate the institution in better understanding the fundamental human rights principles, frameworks and international best practices to be adopted on key concepts such as the right to privacy and personal data protection in Pakistan.

Introduction

The Universal Declaration of Human Rights (UDHR)[1] is a seminal document created in 1948 as a 'common standard of achievements for all peoples and all nations'. Article 12 of the UDHR recognizes the right to privacy as one of the 30 core human rights of which all human beings are deserving.

In the context of Pakistan, the Constitution of the country[2] through Article 14 recognizes privacy and dignity of man as inviolable.

The status of privacy as a fundamental right is unquestionable given the impact its violation can and does have on any individual or populace.

The impact of digitization has been seen through various lens and has affected almost every aspect of everyday life.

The online-offline continuum has highlighted the many harms that can shift from one space to another almost instantaneously and seamlessly.

What we do in our online lives is no longer separate from what is commonly referred to as our ‘real lives’.

Given this, the protection of personal information is an urgent and imperative priority in today’s world. Pakistan does not yet have a law governing data protection however the Personal Data Protection Bill of 2023[3] proposed by the Ministry of Information Technology and Telecommunication (MoITT) is the current blueprint for what may soon become the law and regulate the use of personal data by data controllers and processors. This booklet expands on the basics of key data protection elements, especially in light of the proposed legislation.

What is data?

Data is information, specifically, factual information. Our own data is referred to as personal data and can cover a wide range of information, as detailed in the next heading.

In today's digitized world, our data is perceived as the most precious commodity[4] and for good reason. It is able to give away a lot about us and in the event of the misuse of such information, the ramifications can be considerable.

The effect of potential data leakages, especially where personal information is at stake, can be particularly advanced if those impacted belong to historically marginalized groups, such as racial, ethnic, gender and religious minorities, women, minors etc.

Being the owner of any data that is collected, stored and/or otherwise utilized makes the person a data subject.

> As per the Personal Data Protection Bill s.2 (j) "data subject" means a natural person who is the subject of the personal data;

What is personal data?

Personal data refers to any information about an individual that is not publicly accessible and should be kept confidential to protect the individual's privacy. This can include many forms of data, those defined in the Personal Data Protection Bill 2023 are laid out below:

Type of data	Definition under Personal Data Protection Bill 2023
Personal data	s.2(z) "personal data" means any information that relates directly or indirectly to a data subject, who is identified or identifiable from that information or other information in the possession of a data controller and/or data processor, including any sensitive or critical personal data. Provided that anonymized, or pseudonymized data which is incapable of identifying an individual is not personal data;
Critical personal data	s.2(g) "critical personal data" means such personal data retained by the public service provider - excluding data open to the public - as well as data identified by sector regulators and classified by the Commission as critical or any data related to international obligations;

Anonymized data	s.2(a)“anonymized 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;
Health data	s.2(q) “health data” means any personal data related to the physical or mental health of a data subject including the recordings regarding the past, present, or future state or provision of health care services, which may reveal information about his health status;
Biometric data	s.2(c)“biometric data” means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a person, which allow or confirm the unique identification of that person, such as facial images or dactyloscopic data;
Sensitive personal data	s.2(kk) “Sensitive personal data” means any personal data relating to: (i) financial information excluding identification number, credit card data, debit card data, account number, or other payment instruments data; (ii) health data (physical, behavioural, psychological, and mental health conditions, or medical records); (iii) computerized national identity card or passport; (iv) biometric data; (v) genetic data; (vi) religious beliefs; (vii) criminal records; (viii) political affiliations; (ix) caste or tribe; (x) individual’s ethnicity;

Protecting personal data is essential to preventing identity theft, fraud, personal risk and unauthorized access to personal and sensitive information. This is why it's important to be aware of what constitutes personal data and take steps to safeguard it both offline and online.

What is privacy?

Privacy is the concept that allows an individual to preserve their information and personal lives to themselves. As per Privacy International, it is a fundamental right that serves as the foundation upon which many other human rights are built.[5] This is precisely what makes it so important. The right to privacy is intrinsically linked to the right to dignity, as ensuring the former allows for the latter to be maintained.

Information privacy, in particular, is the right to have some control over how an individual's personal information is collected and used. It is a fundamental human right that everyone has, regardless of their class, race, age, gender or any other identity marker.

Legally, the right to privacy is granted to the citizens of Pakistan through Article 14 of the Constitution.

If looking at international definitions, as per the Office of the Australian Information Commissioner,[6] the right to privacy generally entails the right:

a. to be free from interference and intrusion,

b. to associate freely with whom you want, and

c. to be able to control who can see or use information about you.

What is consent?

Consent is a concept that does not have one definition and its understanding can vary depending on the situation, location and law of the country in question.

Generally, consent is the wilful acceptance of a given statement, intent or action, depicting the agreement of the individual in front of whom the proposition is laid out.

Contract Act of 1872	Personal Data Protection Bill 2023
s.13."Consent" defined. Two or more persons are said to consent when they agree upon the same thing in the same sense.	s.2(f) "'consent" means any freely given, specific, informed, and unambiguous indication of the data subject's intention by which the data subject by a statement or by clear affirmative action, signifies agreement to the collecting, obtaining, and processing of personal data provided that it conforms with section 13 and 14 of the Contract Act, 1872;'

It is crucial to note that consent is not just verbalized or indicated per se, but freely given, informed and unambiguous[7] and that there is an absence of coercion, fraud or error[8] in the equation.

What is the age of majority and minority?

According to the Amendment in the Majority Act 1875,[9] "every person domiciled in Pakistan is deemed to have attained his majority when he shall complete his age of 18 years and not before".

There has not been any update on this definition since. Therefore the age of majority in Pakistan is set at 18 years old. The age of minority is any age up till 17 years of age.

Special provisions for minors

Many social media platforms have introduced special provisions for minors on their platform.[10]

The key resources have been added below:

Application, Platform or Website	Provision
Meta (Facebook, Instagram, WhatsApp):	Meta has slightly different teen safety rules per app: • Those under the age of 16 are defaulted to more private settings on Facebook. • Age verification and detection, through AI to provide age appropriate experiences. • Limited ad targeting and they can use quiet mode to get off the apps for a while.
Twitter/X:	Twitter requires all users to be at least 13 years old, but in some countries, parents or guardians will need to provide consent on the child's behalf to process their personal data.
Snapchat:	Snap introduced an in-app tool called "Family Centre" where parents, guardians, or trusted relatives aged 25 and over can be invited to join with related teens between 13 and 18 years old to have more insight into who the teens are friends with and who they have been chatting with in the past seven days, without revealing any of the specific content of those conversations.

Tiktok:	TikTok accounts registered to existing and new users aged between 13 and 15 years old are private by default and direct messaging is only possible for those aged 16 and older.
Pinterest:	Teen accounts under 16 are now private by default and age verification is part of their policies.
YouTube:	It has two options for accounts for children; a supervised account on YouTube and the YouTube Kids app. In the latter option, parents can customize what content kids can and cannot see and set a screen time limit on the app.
Take It Down:	The National Center for Missing and Exploited Children launched a tool (https://takeitdown.ncmec.org/) to combat children and young people's intimate picture abuse. The tool creates a hash of nude, partially nude, or sexual images or videos that is then used to stop the sharing of such images on partner platforms which includes major social media sites/apps.

Difference between the private and public spheres

The public sphere includes areas where individuals' activities and communications are openly accessible to others, such as social media platforms, public websites, and forums. Information shared in these spaces is generally considered accessible to the public and subject to different privacy expectations compared to private communications.[11]

Private space, however, includes areas where individuals conduct their personal, confidential activities, such as private emails, encrypted messages, and personal data stored on secure devices.[12]

Who are data processors and data controllers?

Data is collected, processed and stored by several actors through digital means. When a user visits a website, for instance, browsing data is generated and collected regarding what is visited, how much time is spent there and what is clicked on. Anyone who collects, stores or analyses that browsing data is a data collector.

It is important to know that data collectors can be the government, private social media companies such as Facebook or Twitter, etc as well as any companies requiring personal data in order to provide services. These are data collectors that collect data largely through legal means, by employing consent. But some people use illegal means, such as hacks or

data leaks, to collect data.

Data holders are persons or organizations who either store personal user data or that data has been shared with them. Data holders can be both data collectors or third parties with whom this personal information is shared.

The Personal Data Protection Bill 2023 recognizes two entities as dealing with data:

> S.2 (h) “data controller” means a person or the government, who either alone or jointly has the authority to decide on the collection, obtaining, usage, or disclosure of personal data;

> S.2 (i) “data processor” means a person or the government who alone or in conjunction with other(s) processes data on behalf of the data controller;

Why is data protection important?

Technological advancement results in all the more progress in the digital domain. However, it also means that technology bears the potential of becoming increasingly invasive.

It is important to have private information as it allows individuals to have agency over their data. With technology becoming ever more invasive, the threat of data being compromised also increases. Therefore, it is important to ensure that their data is protected. Recent examples of data breaches, such as those at the National Database and Registration Authority (NADRA) and the Federal Investigation Agency (FIA),[13] Dar-ul-Aman Rawalpindi[14] and the Safe City Authority,[15] have brought into light the various ways in which citizens' data can be compromised and misused.

On an international level, the Cambridge Analytica data scandal highlighted the impact of data mining on democratic processes. A journalistic probe[16] brought to light the use of improperly obtained data of millions of Facebook users to build voter profiles and influence the U.S presidential election in 2016.[17]

As technology becomes more integrated into our lives, with personal data now stored on various devices, it is crucial to implement strong data protection measures. Both individuals and companies, whether public or private, must ensure the safety of this data.

Data autonomy

The concept of autonomy is deeply rooted in our constitutional framework, which guarantees individuals the right to bodily autonomy and integrity. This fundamental right ensures that individuals have control over their physical selves, free from unwarranted intrusions or violations. Similarly, the autonomy over one's data mirrors this constitutional protection of physical privacy, affirming that citizens have the right to control access to their digital information and communications, just as they do with their physical selves. This principle has been expounded upon in the case of Muhammad Rahmat Ullah vs. The State,[18] wherein the recognition of data autonomy as a fundamental right enables individuals to exercise control over their digital footprint and make informed decisions regarding the use of their personal information.

Tech-facilitated gender based violence (TF-GBV)

Violations of privacy are exacerbated across gender lines.

As DRF's White Paper: A Southern and Southeast Asian Lens on Online Harms,[19] states, gender-based violence consists of harmful acts directed at an individual, based on their gender. Certain individuals are at a higher degree of risk of facing violence, simply due to their gender.

It defines tech-facilitated gender-based violence (TF-GBV) as 'the use of internet and digital platforms to inflict, assist in inflicting or aggravating violence on women and gender and sexual minority community members (including transgender, non-binary, queer individuals)'

In March of 2020, the United Nations Special Rapporteur on the right to privacy, Joseph Cannataci, called for gender equality to be embedded in privacy practices around the world.

An excerpt from his report states:

> *Reports of harm arising from gender-based infringements of privacy include serious, well-documented effects. Violence and even death were consequences reported in submissions.*[20]

Taking it forward from there, the impact of data violation is significantly harsher on the marginalized end of the gender spectrum, from increased discrimination to amplification of existing threats and risks to personal and communal safety. Thus, the protection of privacy becomes a life-saving priority in such instances and should be treated as such.

Pakistani jurisprudence on privacy:

Mohtarma Benazir Bhutto vs. President of Pakistan (P L D 1998 Supreme Court 388)

Summary: In this landmark case, the Supreme Court of Pakistan examined the legality of telephone tapping and eavesdropping under Article 14 of the Constitution. The case involved allegations against Prime Minister Benazir Bhutto's government for unlawfully tapping phones of judges, political leaders, and military officers. The Court ruled that such actions violated the inviolable rights to dignity and privacy, extending beyond physical spaces to include public places.

Relevant Excerpt: "The inviolability of privacy is directly linked with the dignity of man. If a man is to preserve his dignity, if he is to live with honour and reputation, his privacy whether in home or outside the home has to be saved from invasion and protected from illegal intrusion. The right conferred under Article 14 is not to any premises, home or office, but to the person, the man/woman wherever he/she may be." (Para 30)

Manzoor Ahmad vs. The State (1990 MLD 1488)

Summary: Invasion of privacy through eavesdropping, tapping, and photographing inside the house is prohibited under Article 14 of the Constitution of Pakistan and is not permissible in Islam.

Relevant Excerpt: "In view of Article 14 of the Constitution Eavesdropping, tapping stealthily, photographing something inside the house are invasions on privacy and as such is not permissible under the Constitution as well as in Islam." (Para 5)

Muhammad Nawaz vs. Additional District and Sessions Judge (P L D 2023 Supreme Court 461)

Summary: Unauthorized DNA collection violates privacy, autonomy, and freedom. The need for protecting personal information from unwarranted intrusion was discussed within the same. Article 14 of the Constitution elevates privacy as a fundamental right, safeguarding individuals' choices and personal lives beyond their physical homes. Privacy is essential for personal autonomy and self-determination.

Relevant Excerpt: "The right to privacy involves the protection of individuals from unwarranted intrusion into their personal lives. It safeguards an individual's personal information, communications, family life, and other aspects of their private sphere from unjustified interference by the government, organizations, or other individuals. Privacy is crucial for

maintaining personal autonomy, as it allows individuals to make choices and engage in activities without fear of surveillance, judgment, or unauthorized disclosure of their personal information." (Para 6)

Summary: Invasion of privacy through eavesdropping, tapping, and photographing inside the house is prohibited under Article 14 of the Constitution of Pakistan and is not permissible in Islam.

Rights of a data subject

As per the draft Personal Data Protection Bill 2023, the key rights of a data subject include:

Right to access under the PDPB 2023, s.16, allows a data subject to confirm whether their personal data is under processing or has been processed by their data controller. The data subject may also (on the payment of a prescribed fee) make a written data access request to the data controller on the status of processing and also ask for a copy of their data.

Right to correction under the PDPB 2023, s.19, is the right where if the personal data of a data subject is inaccurate, incomplete, misleading, or not up to date in their estimation, the data subject may make a data correction request in writing to the data controller to make the necessary corrections.

Right to erasure under the PDPB 2023, s.26, is the right of a data subject to request the erasure of his personal data and the obligation to do so within 14 days lies with the data controller if:

(a) the personal data is no longer necessary concerning the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based under sub-section (1) of section 23 (right to withdrawal of consent) and where there is no other legal ground for the processing; or
(c) the data subject objects to the processing under sub-section (2) of section 23;
(d) the personal data have been unlawfully processed; or
(e) the personal data must be erased for compliance with a legal obligation

Right to nominate under PDPB 2023, s.27, is the right of the data subject to nominate, any other individual as may be prescribed, to exercise the rights of the data subject under the provisions of this Act, in the event of the death or disability of the data subject.

Right to redressal and grievance under PDPB 2023, s.28, is the right of the data subject to be provided with means to register his complaint in writing with a data controller, in case of any complaint/grievance. The data controller officials shall immediately take up the matter for redressal.

In the case where a data controller fails to satisfy a data subject with a satisfactory response concerning a grievance or receives no response within the prescribed period, he may register a complaint with the National Commission for Personal Data Protection (NCPDP) in such manner as may be prescribed.

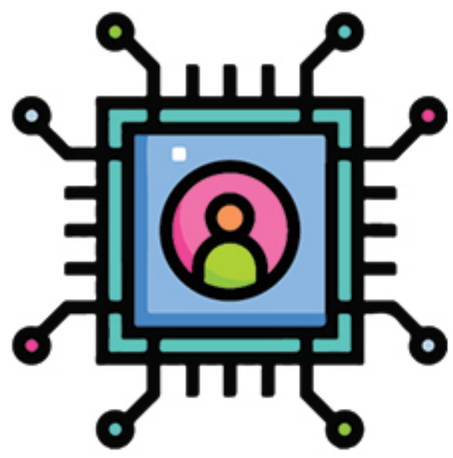
Right to data portability and automated processing under PDPB 2023, s.29 is the right of the data subject to receive his personal data from a data controller in a proper form, that is easy to use and in a machine-readable format, and the data subject shall have the right to transmit that data to another data controller or processor without any objection where:
(a) the data subject has given his explicit consent; and
(b) the processing is carried out by automated means.
With the exception of processing of data for the purposes of public interest.

Secondly, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which results in legal obligations or significantly harms the data subject, unless the data subject has given his explicit consent. Additionally, the data subject shall have the right to obtain from the data controller:

(a) specific information about automated decision-making including profiling,

(b) human intervention

The implications of digital identity



Some individuals mistakenly believe that once they delete content from social media, it is gone forever. This is not the case. Even if a website or post is removed, online caches often retain those entries, meaning nothing shared online is truly private.

Meta Data [21]	**Caches** [22]	**Cookies** [23]
Metadata is data that provides information about other data. It includes details such as the author, date created, date modified, file size, and more, which helps in organizing, finding, and understanding the data.	A cache is a hardware or software component that stores data so that future requests for that data can be served faster. The data stored in a cache might be the result of an earlier computation or a copy of data stored elsewhere.	Cookies are small pieces of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing. They are designed to be a reliable mechanism for websites to remember stateful information or to record the user's browsing activity.

It is important to exercise caution with the information people share online and it is a good practice to regularly search one's name on search engines to monitor personal information that may have been shared without consent. Every online action leaves a traceable digital footprint,[24] which websites collect to identify, track, and commodify users, often selling this data to advertisers. Social media platforms like Meta and various free online applications, including those for social media, gaming, delivery, and entertainment, access and collect data from mobile phones. It is important to review app permissions carefully to understand the data that is being shared.

Growing digitization and its impact on privacy

In Pakistan, the rapid growth of digitization has significantly changed interactions, business conduct, and daily management, but it has also raised privacy and data security concerns. The easy accessibility of personal information online increases vulnerability to cybercrime, with stolen data often sold on the Dark Web.[25] Using the same password across multiple sites heightens the risk of cyberattacks, potentially leading to financial losses and identity theft. To protect personal information, individuals should regularly update passwords, monitor their online presence, and be cautious about sharing personal data.

Term	Definition	PDPB Definition	Distinction
Data Breach [26]	A data breach is an incident where unauthorized individuals gain access to confidential, sensitive, or protected data. This can result from cyberattacks, hacking, or theft.	S.2 (aa) "personal data breach" means 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;"	Involves deliberate and malicious action to obtain data, often through cyberattacks or hacking.

Term	Definition	PDPB Definition	Distinction
Data Leak[27]	A data leak is an incident where sensitive information is unintentionally exposed to the public or unauthorized parties, often due to internal errors, misconfigurations, or negligence.	There is no definition given in the draft.	Occurs unintentionally, often due to errors or negligence, leading to accidental exposure of sensitive information.

Conclusion

The right to privacy, through various international treaties, instruments and national and regional frameworks is established as a fundamental human right to be afforded to all human beings. Pakistan is a democratic nation that awards the same to its citizens, however the advances in technology, the floodgate of data consumption and protection and the lack of a transparent and comprehensive data protection regime puts the citizens of the country at risk.

The judiciary, as one of the most crucial organs of State, owes a significant responsibility to the citizens of Pakistan to take note of the brewing crisis around personal data, irresponsible practices and lack of oversight and establish precedent championing the rights to dignity and privacy.

Bibliography

حوالہ جات

1. https://www.un.org/en/about-us/universal-declaration-of-human-rights

2. https://www.pakistani.org/pakistan/constitution/

3. https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf

4. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

5. https://privacyinternational.org/explainer/56/what-privacy

6. https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-privacy#:~:text=Generally%20speaking%2C%20privacy%20includes%20the,or%20use%20information%20about%20you.

7. https://gdpr-info.eu/issues/consent/

8. https://www.law.cornell.edu/wex/consent#:~:text=Consent%20means%20that%20a%20person,of%20coercion%2C%20fraud%20or%20error.

9. http://www.ljcp.gov.pk/Menu%20Items/Reports_of_LJCP/09/90.pdf

10. https://the-media-leader.com/how-do-social-media-platforms-teen-and-parental-control-policies-compare/

11. https://mitpress.mit.edu/9780262581080/the-structural-transformation-of-the-public-sphere/

12. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888

13. https://www.dawn.com/news/1824026

14. https://tribune.com.pk/story/2469054/probe-uncovers-secret-cameras-in-womens-shelter-in-rawal

15. https://www.dawn.com/news/1835677

16. https://bipartisanpolicy.org/blog/cambridge-analytica-controversy/#:~:text=On%20March%2017%2C%202018%2C%20the,everything%20on%20Facebook%20for%20Cambridge

17. https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/

18. Muhammad Rahmat Ullah vs. The State (2024 PCR.LJ 1).

19. https://digitalrightsfoundation.pk/wp-content/uploads/2024/05/White-Paper-A-Southern-and-Southeast-Asian-lens-on-Online-Harms.pdf

20. https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/StatementHRC_40_Privacy.pdf

21. https://guides.library.cmu.edu/Metadata#:~:text=Definition%20from%20the%20National%20Information,or%20manage%20an%20information%20resource.%22

22. https://developer.mozilla.org/en-US/docs/Web/HTTP/Caching

23. https://www.ietf.org/archive/id/draft-ietf-httpbis-rfc6265bis-07.html

24. https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

25. https://www.sciencedirect.com/science/article/pii/S0167404824001275

26. https://www.ibm.com/topics/data-breach

27. https://media.techtarget.com/searchCIO-Midmarket/downloads/databreach_ebook.pdf