BOLO BHI
Advocacy - Policy - Research

COMPARATIVE ANALYSIS OF PERSONAL DATA PROTECTION BILL 2020 WITH LAWS AND BILLS IN THE EU, UK, INDIA & MALAYSIA

www.bolobhi.org

Table of Contents

Overview of the Comparative Analysis

By Shumaila Hussain Shahani

The draft Personal Data Protection Bill, 2020 was made available by the Ministry of Information Technology and Telecommunication (MoITT) on its website on April 9, 2020. This analysis compares the draft Personal Data Protection Bill 2020 to the General Data Protection Regulation (GDPR) (from which the draft Bill draws extensively), the Malaysian Personal Data Protection Act 2010, the UK's Data Protection Act (DPA), 2018, and India's Personal Data Protection Bill 2019 which is currently being debated by a Joint Parliamentary Committee in consultation with various groups. The purpose of the comparison is to analyse the differences and commonalities, explore if there are best practices that should be adopted, and consider safeguards for rights that should be incorporated in Pakistan's draft Personal Data Protection Bill, 2020.

Under the draft Personal Data Protection Bill 2020, the Authority set up functions under the Federal Government administratively. The Federal Government can appoint members – one of them an ex-officio member of a Ministry – who function as employees of the Authority and are to be paid salaries through a Fund set up and money contributed by the Federal Government. Similar provisions are found in the Malaysian Personal Data Protection Act 2010 and Indian Personal Data Protection Bill 2019. The Indian Personal Data Protection Bill 2019 authorizes the Central Government to issue directions to the Authority as it deems necessary, while the Malaysian Personal Data Protection Act 2010 allows the Minister to appoint any person as the "Personal Data Protection Commissioner" on such terms and conditions as he thinks desirable.

As Bolo Bhi's analysis of the Personal Data Protection Bill 2020 points out, the Authority set up under the draft lacks independence and autonomy. Comparable provisions that exist in the Indian Personal Data Protection Bill 2019 and Malaysian Personal Data Protection Act 2010 are equally problematic as they create room for wide discretion and little external accountability, leaving

data at the disposal of governments and officials appointed by them. Centre for Internet and Society in India, critiqued the composition of the members of the selection committee, responsible for the selection of members of the authority, arguing that it compromises on the independence of the Authority. It further said that "for an efficient and smooth functioning of the Authority, it is necessary that the members of the Authority are able to function in an independent manner and are insulated from government control". The lack of independence of the Commissioner under Malaysian Personal Data Protection Act 2010 has been highlighted by critics of the Act on several occasions calling for a need for an independent supervisory authority. Instead of emulating these examples, guidance should be taken from Article 52 of the GDPR, which requires supervisory authorities to perform tasks and exercise powers independently, and members are required to remain free of external influence, whether direct or indirect, and refrain from taking instructions from others. As in the UK, where the DPA 2018 gives the existing Information Commission mandate under the law, an independent, statutory commission (which currently does not exist in Pakistan), should be created instead of setting up an Authority that functions under the Federal Government.

At present, the draft Personal Data Protection Bill 2020 exempts the gathering and use of personal data by law-enforcement agencies for the purposes of the prevention, investigation, detection or prosecution of criminal offences. Collection, storage and use of data by intelligence agencies is also not covered. The Bill also allows the federal government to grant further exemptions in a discretionary manner. The GDPR does not deal with data processing for law enforcement purposes however, the UK DPA 2018 regulates processing of data by law-enforcement agencies by implementing Law Enforcement Directive (LED) in Part 3 of the Act. Data processing by intelligence agencies in Part 4 of the Act. Germany's Federal Constitutional Court on May 19, 2020 subjected German spy agency, Bundesnachrichtendienst (BND) to provisions under the German Constitution by ruling that "the German state authority is bound by the fundamental rights of the Basic Law (German constitution), not only within the German territory," declaring BND's surveillance and monitoring of telephones and internet data of foreign nationals residing outside the territorial jurisdiction of Germany unconstitutional for

being in violation of the rights of freedom of the press and privacy in telecommunications enshrined in the German Constitution. The court held that Article 1 (3) of the Constitution binds the BND to respect fundamental human rights including Article 5 (1) freedom of expression and Article 10 (1) right to privacy regardless of whether the operations are conducted inside the German territory or outside. The petitioners, investigative journalists and human rights activists from various countries supported by the the German Journalists' Union/dju, the German Federation of Journalists, the journalists' network n-ost, netzwerk recherche (nr) (research network) and Reporters without Borders, had challenged amendments made to the Federal Intelligence Service Act 1990 in 2017 allowing the BND to collect, gather and process data about foreign nationals residing outside the territorial jurisdiction of Germany, "without the agency having to provide legal justification."

The exemptions to the prohibition of processing of "personal data" including "sensitive personal data" in all jurisdictions reviewed for the purpose of this comparison, are too broad. The European Court of Human Rights (ECHR) rulings in Malone versus United Kingdom 1984 and Zakharov versus Russia 2015 should be considered in this regard. In the 1984 ruling, the ECHR held that UK Metropolitan Police Commissioner's interception of the applicant's telephone conversations on authority of a warrant by the Secretary of State for Home Affairs was not "in accordance with the law" and in breach of Article 8 of the European Convention on Human Rights, which deals with right to privacy. In the 2015 ruling, the ECHR once again held that Russia's legal provisions governing communications surveillance violated Article 8 of the European Convention on Human Rights as they did not provide adequate safeguards against arbitrariness or abuse. The ECHR, in these judgments, recognised the need to access data in serious criminal offences, but provided protections and safeguards, subjecting it to the reasoned decisions and authorization of courts. Both the UK and Russia have since, overturned the impact of these decisions within their jurisdictions and have instead legalised privacy invasions through various legislations further enabling widespread powers to intercept, surveil, and store personal data.

In recent years, the European Court of Justice (ECJ) held in December 2016, that the Data Retention and Investigatory Powers Act 2014 (DRIPA) was unlawful and violated privacy rights guaranteed under the Charter of Fundamental Rights of the European Union (CFR). DRIPA was legislated in response to the ECJ's 2014 ruling declaring the Data Retention Directive invalid as the Directive "entailed serious interference with rights to privacy and personal data protection" of individuals in violation of rights guaranteed by the CFR. The Investigatory Powers Act 2016, commonly known as Snoopers' Charter by its critics, was enacted to replace DRIPA, however the law continues to face criticism and challenges for being violative of EU laws.

Over years as data leaks, breaches and extent of surveillance have become public knowledge, it is all the more important that the definitions of "data controller" and "data processor" include public authorities, law-enforcement and intelligence agencies, and any other body that collects, stores and processes data. Hence the exemption in the draft Personal Data Protection Bill 2020, permitting the processing of sensitive and non-sensitive personal data for the prevention, detection, investigation of crime, or to apprehend and prosecute offenders, should be regulated, allowed only for specific serious criminal offences, subjected to warrants based on reasoned orders by courts.

The grounds for processing "sensitive personal data" in the draft Personal Data Protection Bill 2020 in exercise and performance of any right or obligation conferred or imposed by law on the "data controller" in connection with employment needs further clarification to determine under what circumstances a person's "sensitive personal data" may be required by their employers and to some degree possible, be specified in the Bill. Currently, the draft Personal Data Protection Bill 2020 does not list the obligations that may be imposed upon a "data controller" to process the "data subject's" sensitive personal data without their consent. The GDPR imposes such a duty on the "data controller" in connection with his employment. Member states are required to provide for appropriate safeguards for the fundamental rights to protect the rights of a "data subject." An even better approach is adopted in the Indian Personal Data Protection Bill 2019, Section 13 of which stipulates that the processing of data for the purposes of employment must

exclude processing of "sensitive personal data," where the consent of the data subject is not taken, bearing in mind the employment relationship between the "data controller" and the "data subject." Political affiliation (including trade-union membership, political party / social movement membership, and other memberships of similar nature), racial origin (including in cases of immigrants and refugees), genetic data, philosophical beliefs, gender status, sex life, or sexual orientation are not covered or protectected categories in the draft Personal Data Protection Bill 2020. These have been included as special categories of personal data in GDPR and the UK DPA 2018, and as "sensitive personal data" in the Indian draft Personal Data Protection Bill 2019.

The draft Personal Data Protection Bill 2020 refers to owners of personal data as "data subject" and those holding personal data as "data controllers" and "data processors." The word "subject" has a negative connotation attached to imply people placed under authority or control by force and such references should be avoided in this day and age. The use of terms such as "data subject" and "data controller" should be reconsidered and substituted instead with "data principal" and "data fiduciary" which appear in the Indian draft Personal Data Protection Bill 2019. The bill is also silent on the processing of data of immigrants and refugees. Article 4 of the Constitution of Pakistan protects the right of individuals to be dealt in accordance with law and Article 14 protects dignity and privacy of every man, not just a citizen. The Germany's Federal Constitutional Court, on May 19, 2020, by binding its spy agency to respect constitutional rights with regards to its activities concerning non-citizens residing and operating outside its territorial boundaries, has extended constitutional protections of the right of freedom of the press and right to privacy to such persons. Among the grounds for processing of personal data mentioned in the draft Personal Data Protection Bill 2020, "vital interests" of the "data subject" and for pursuance of "legitimate interests" by the "data controller" are far too vague. Similar grounds for processing exist in GDPR, the UK DPA and Malaysian Personal Data Protection Act 2010. This suggests adults are unable to protect their own vital interests, provide consent for the protection of their vital interests, or decide which interests are vital to them. What are "legitimate interests" that a "data controller" may need to pursue as they have not been explicitly defined in the draft

Personal Data Protection Bill, 2020.

In order for the Personal Data Protection Bill 2020 to effectively protect data and rights, it should not be vague, cover all sectors and entities, refrain from awarding discretionary powers especially to make broad exemptions to chosen entities.

COMPARISON

1. Scope of the Laws

1.1. *Definitions*

The definition section of draft Personal Data Protection Bill, 2020 covers only some of the major terminologies while several others as defined in other legislations are missing. For example, GDPR also defines and covers "genetic data", "biometric data", "data concerning health" etc. "Restriction of processing" and "personal data breach" also remain undefined in the draft Personal Data Protection Bill 2020. Under the UK's DPA 2018, the terms used in the Act mainly have the same meanings as they have in the GDPR.

The definitions section of the Indian Personal Data Protection Bill 2019 provides definitions for the following important terms not covered or defined by the draft Personal Data Protection Bill, 2020: 1) Adjudicating Officer, 2) Anonymisation, 3) Appellate Tribunal, 4) Automated, 5) Biometric data, 6) Child, 7) Code of practice, 8) Data, 9) Data auditor, 10) Data fiduciary, 11) Data principal, 12) De-identification, 13) Disaster, 14) Financial data, 15) Genetic data, 16) Harm, 17) Health data, 18) Intra-group schemes, 19) In writing, 20) Journalistic purpose, 21) Notification, 22) Official identifier, 23) Personal data breach, 24) Prescribed, 25) Profiling, 26) Regulations, 27) Re-identification, 28) Significant data fiduciary, 29) Significant harm, 30)

Systematic activity.

Section 4 of the Malaysian Personal Data Protection Act 2010 provides definitions for the following important terms not covered/defined by the draft Personal Data Protection Bill, 2020: 1) Credit reporting agency, 2) This Act, 3) Register, 4) Prescribed, 5) Advisory Committee, 6) Fund, 7) Use, 8) Collect, 9) Minister, 10) Disclose, 11) Authorized officer, 12) Correction, 13) Requestor, 14) Registration, 15) Relevant data user, 16) Credit reporting business, 17) Commissioner, 18) Relevant filing system, 19) Appointed date, 20) Code of practice, 21) Commercial transactions.

The terms "data subject", "data controller" and "data processor" in the draft Personal Data Protection Bill, 2020 are referred to as "data subject", "controller" and "processor" respectively in GDPR, referred to as "data subject", "data user" and "data processor" in the Malaysian Personal Data Protection Act 2010 and are referred to as "data principal", "data fiduciary" and "data processor" in the Indian Personal Data Protection Bill 2019. The definition of "data subject" in the draft Personal Data Protection Bill, 2020 is almost similar to the definitions given to the term in all the other jurisdictions mentioned here. However, the definitions of "data controller" and "data processor" in the draft Personal Data Protection Bill, 2020 do not include public authorities, agencies, or any other body that collects, stores and processes data, in addition to natural or legal persons as defined in GDPR.

It is recommended that the draft Personal Data Protection Bill 2020 should at least add to its definitions 1) Anonymisation, 2) Biometric data, 3) Genetic data, 4) Health data, 5) Personal data breach, 6) Critical Data breach, 7) Sensitive Data breach, 8) Profiling, 9) Harm, 10) Significant harm, 11) Correction, 12) Erasure, 13) Restriction of processing.

1.2. *Application of the Laws*

The draft Personal Data Protection Bill, 2020 applies to any person who processes or has control

over or authorizes the processing of any personal data, provided any of the "data subject", "controller", or "processor" (either local or foreign) is located in Pakistan.

Article 2 of the GDPR defining material scope of the GDPR states that the Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. However, it does not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law; or by the Member States when carrying out activities which fall within the scope of specific provisions on the common foreign and security policy as defined in Chapter 2 of Title V of the TEU; or by a natural person in the course of a purely personal or household activity; or by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. It further states that for the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 is a regulation "on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data". Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98 under which the Commission is authorized to submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

The UK DPA 2018 applies to general processing, processing by law enforcement and processing by intelligence agencies. According to the Section 4 of the DPA 2018, general processing includes the types of processing of personal data to which the GDPR applies by virtue of Article 2 (material scope) of the GDPR, and also applies to certain types of processing of personal data to which the GDPR does not apply, and makes provision for a regime broadly equivalent to the

GDPR to apply to such processing. Its Section 21 explains certain types of processing of personal data which is covered by the DPA 2018 but not covered by the GDPR. It includes automated or structured processing of personal data in the course of an activity which is outside the scope of European Union law, or an activity which falls within the scope of common foreign and security policy activities as defined in Article 2(2)(b) of the GDPR It also applies to the manual unstructured processing of personal data held by an FOI (Freedom of Information) public authority, however it does not apply to the processing of personal data by an individual in the course of a purely personal or household activity.

Section 29 of the UK DPA 2018 deals with processing by law enforcement. It applies to the processing by a competent authority of personal data wholly or partly by automated means, and the processing by a competent authority otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system. Section 82 of the UK DPA 2018 deals with processing by intelligence agencies and applies to the processing by an intelligence service of personal data wholly or partly by automated means, and the processing by an intelligence service otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system.

The Malaysian Personal Data Protection Act 2010 applies to any person who processes; and any person who has control over or authorizes the processing of any personal data in respect of commercial transactions or to a person in respect of personal data if the person is established in Malaysia and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or the person is not established in Malaysia, but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia. The Malaysian Personal Data Protection Act 2010 does not apply to the Federal Government and State Governments or to any personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia.

The Indian Personal Data Protection Bill 2019 applies to the processing of personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India; the processing of personal data by the State, any Indian company, any citizen of India or any person or body of persons incorporated or created under Indian law, the processing of personal data by "data fiduciaries" or "data processors" not present within the territory of India, (if such processing is in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or is in connection with any activity which involves profiling of data principals within the territory of India). The Indian Personal Data Protection Bill 2019 does not apply to the processing of anonymised data, other than the anonymised data referred to in section 91.

1.3. *Grounds for Processing of Personal Data*

The UK's DPA 2018 allows data processing only for the purposes of the administration of justice, the exercise of a function of either House of Parliament, the exercise of a function conferred on a person by an enactment or rule of law, the exercise of a function of the Crown, a Minister of the Crown or a government department, or an activity that supports or promotes democratic engagement.

However, Pakistan's draft Personal Data Protection Bill 2020 goes much further, and allows processing of personal data for the performance of a contract to which the "data subject" is a party, for taking steps at the request of the "data subject" with a view to entering into a contract, for compliance with any legal obligation to which the "data controller" is the subject, other than an obligation imposed by a contract, in order 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 the exercise of any functions conferred on any person by or under any law.

Article 6 of GDPR states that processing shall only be lawful where the "data subject" has given

consent; or processing is necessary for the performance of a contract to which the “data subject” is party or in order to take steps at the request of the “data subject” prior to entering into a contract; or processing is necessary for compliance with a legal obligation to which the "controller" is subject; or processing is necessary in order to protect the “vital interests” of the “data subject” or of another natural person; or processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the "controller"; or processing is necessary for the purposes of the “legitimate interests” pursued by the "controller" or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the “data subject” which require protection of personal data, in particular where the “data subject” is a child. Requirement for processing in pursuance of “legitimate interests” does not apply to processing carried out by public authorities in the performance of their tasks. GDPR states that Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing. It further states that the basis for the processing with regards to legal obligation subjecting the "controller" and in performance of a task carried out in public interest shall be laid down by Union law; or Member State law to which the "controller" is subject. It holds that the Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

Article 6 of the GDPR further states that where the processing for a purpose other than that for which the personal data have been collected is not based on the “data subject’s” consent or on a Union or Member State law, the "controller" shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; the context in which the personal data have been collected, in particular regarding the relationship between “data subjects” and the "controller"; the nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed; the possible consequences of the intended further

processing for “data subjects”; and the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Section 2 and Section 3 of the Malaysian Personal Data Protection Act 2010 state that the Act applies to any person who processes; and any person who has control over or authorizes the processing of any personal data in respect of commercial transactions. This Act does not apply to the Federal Government and State Governments or to any personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia.

Chapter III of the Indian Personal Data Protection Bill 2019 provides grounds for processing of personal data without consent. These grounds are related to state benefits and health, specifically:

a) the performance of any function of the State authorised by law for the provision of any service or benefit to the data principal from the State.

b) or the issuance of any certification, licence or permit for any action or activity of the data principal by the State or for compliance with any order or judgment of any Court or Tribunal in India or to respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal or any other individual or to undertake any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health or to undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order.

c) Section 13 of the Indian Personal Data Protection Bill 2019 deals with processing of personal data, not being sensitive personal data, necessary for purposes related to employment, etc where the consent of the data principal is not appropriate having regard to the employment relationship between the data fiduciary and the data principal, or would involve a disproportionate effort on the part of the data fiduciary due to the nature of the processing under this section. This includes processing of non-sensitive data if necessary for recruitment or termination of employment of a data principal by the data fiduciary or provision of any service to, or benefit sought by the data principal who is an employee of the data fiduciary or verifying the attendance of the data

principal who is an employee of the data fiduciary or any other activity relating to the assessment of the performance of the data principal who is an employee of the data fiduciary.

d) Section 14 of the Indian Personal Data Protection Bill 2019 deals with processing of personal data for other reasonable purposes as may be specified by regulations, after taking into consideration following considerations: 1) the interest of the data fiduciary in processing for that purpose, 2) whether the data fiduciary can reasonably be expected to obtain the consent of the data principal, 3) any public interest in processing for that purpose, 4) the effect of the processing activity on the rights of the data principal, 5) and the reasonable expectations of the data principal having regard to the context of the processing. The expression "reasonable purposes" is further explained to include prevention and detection of any unlawful activity including fraud; whistle blowing; mergers and acquisitions; network and information security; credit scoring; recovery of debt; processing of publicly available personal data; and the operation of search engines.

1.4. *Sensitive Personal Data*

Section 28 of the draft Personal Data Protection Bill 2020 prohibits the processing of sensitive personal data which is defined as data relating to access control (username and/or password), financial information such as bank account, credit card, debit card, or other payment instruments, and, passports, biometric data, and physical, psychological, and mental health conditions, medical records, and any detail pertaining to an individual's ethnicity, religious beliefs, or any other information for the purposes of this Act and rules made thereunder.

The GDPR in its Article 9 has provided details on processing of special categories of personal data. Under this Article, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation has be prohibited with certain exceptions.

Defined as in the GDPR, the processing of sensitive personal data is dealt with in the DPA 2018 in Schedule 8. Conditions for sensitive data processing are: statutory purposes, administration of justice, protecting individual's vital interests, safeguarding of children and individuals at risk, personal data already in public domain, legal claims, judicial acts, preventing fraud, archiving etc.

In the Malaysian Personal Data Protection Act 2010, "sensitive personal data" is defined as any personal data consisting of information as to the physical or mental health or condition of a "data subject", his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the Gazette.

The conditions for processing of personal data in the draft Personal Data Protection Bill 2020 are copied from the Malaysian Personal Data Protection Act 2010 except the condition in the Malaysian Act which gives the Minister the power to order processing as and when required.

Under the Indian Personal Data Protection Bill 2019, the central government in consultation with the Authority and the sectoral regulator concerned, may notify such categories of personal data as "sensitive personal data", having regard to the risk of significant harm that may be caused to the data principal by the processing of such category of personal data; the expectation of confidentiality attached to such category of personal data; whether a significantly discernible class of data principals may suffer significant harm from the processing of such category of personal data; and the adequacy of protection afforded by ordinary provisions applicable to personal data. The Authority may specify, by regulations, the additional safeguards or restrictions for the purposes of repeated, continuous or systematic collection of sensitive personal data for profiling of such personal data.

The exemptions to Section 28 of the the draft Personal Data Protection Bill 2020, almost copied

form the Malaysian Personal Data Protection Act 2010, include:

1. consent of the "data subject";
2. "data controller" performing any right or obligation conferred in connection with his employment;
3. to protect "vital interests" of "data subject" or another person;
4. for medical purposes;
5. in connection with, any legal proceedings, for the purpose of obtaining legal advice while ensuring its integrity and secrecy;
6. for the purposes of establishing, exercising or defending legal rights;
7. 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 written law; and
8. where the information contained in the personal data has been made public as a result of steps deliberately taken by the "data subject".

Some of these exemptions have been taken from the exemptions provided in the GDPR. The exemption in the GDPR where the "data controller" is required to process data with the duty imposed by law in connection with his employment is specific to data controllers in the field of employment and social security and social protection law, and not any other data controllers.

2. Regulatory Body

The draft Personal Data Protection Bill 2020 deals with the formation of a regulatory body, the Personal Data Protection Authority of Pakistan (Authority) under Chapter VI which will be established by the Federal Government through a notification. The Authority shall be a statutory corporate body having perpetual succession and a common seal, and may sue and be sued in its own name and, subject to and for the purposes of the Act, may enter into contracts and may acquire, purchase, take and hold moveable and immovable property of every description and may convey, assign, surrender, charge, mortgage, reassign, transfer or otherwise dispose of or deal with, any movable or immovable property or any interest vested in it and shall enjoy

operational and administrative autonomy, except as specifically provided for under this Act. The Authority shall be an autonomous body under the administrative control of the Federal government with its headquarters in Islamabad.

Under the UK Data Protection Act, 2018, the Information Commission Office under the Freedom of Information Act 2000 acts as an Authority as provided under Section 7 of the DPA 2018.

Chapter IX of the Indian Personal Data Protection Bill 2019 deals with the formation of a Data Protection Authority of India. Under Section 86, the Central Government has the powers to issue to the Authority such directions as it may think necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order. The Authority shall be a body corporate having perpetual succession and a common seal, with power, subject to the provisions of the Act, to acquire, hold and dispose of property, both movable and immovable, and to contract and shall, by the said name, sue or be sued.

PART IV of the Malaysian Personal Data Protection Act 2010 deals with appointment, functions and powers of commissioners. Under Section 47, the Minister appoints any person as the "Personal Data Protection Commissioner" for the purposes of carrying out the functions and powers assigned to the Commissioner under the Act on such terms and conditions as he thinks desirable. The Commissioner appointed is a body corporate having perpetual succession and a common seal. The Commissioner may sue and be sued in his corporate name.

The GDPR deals with the topic of independent supervisory authorities (detailed in the next section) in its Chapter 6 which under the GDPR have to be established to independently supervise the implementation of GDPR. Article 52 deals with independence of the authority where it states that each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation and members of each supervisory authority shall remain free from external influence, whether direct or

indirect, and shall neither seek nor take instructions from anybody.

2.1. *Yearly Reports*

Article 41 of the draft Personal Data Protection Bill 2020 obligates the Authority to submit yearly reports on its activities to the Federal Government. Such a report along with a copy of the audit report will be then presented to the Parliament within three months.

Article 59 of the GDPR deals with activity reports by the supervisory authorities where they must submit annual reports on its activities, which may include a list of types of infringement notified and types of remedial measures taken to the national Parliament, the Government and other authorities as designated by Member State law. Finland has established "Office of the Data Protection Ombudsman", Hungry has created "National Authority for Data Protection and Freedom of Information" and Ireland has for example established, "Data Protection Commissioner" in compliance with GDPR which after establishment are responsible to carry out tasks assigned to supervisory authorities in GDPR. In the UK, the Information Commissioner's Office is obligated to fulfill this task under the DPA 2018.

Article 59 also states that the reports shall be made available to the public, to the European Commission and to the European Data Protection Board.

The UK's DPA 2018 deals with reporting to the British Parliament in Section 139 under which the Commissioner must produce a general report on the carrying out of the Commissioner's functions annually, arrange for it to be laid before Parliament, and publish it. The report must include the annual report required under Article 59 of the GDPR. The Commissioner may produce other reports relating to the carrying out of the Commissioner's functions and arrange for them to be laid before Parliament.

Section 103 the Malaysian Personal Data Protection Act 2010 deals with reports by the

Commissioner. The Commissioner is required to publish a report setting out any recommendations that the Commissioner thinks fit relating to the promotion of compliance with the provisions of this Act, in particular the Personal Data Protection Principles, by the class of data users to which the relevant data users belong. The report shall be so framed as to prevent the identity of any individual from being ascertained.

Under Section 81 of the Indian Personal Data Protection Bill 2019, the Authority shall prepare once every year in such form and at such time as may be prescribed, an annual report giving a summary of its activities during the previous year and copies of the report shall be forwarded to the Central Government which then shall be laid, as soon as may be after it is received, before each House of the Parliament and shall also be made publicly available by the Authority.

There should be no interference of the Federal government in the publication and production of the Authority's annual report before the Parliament. As observed from the comparison above, no other jurisdiction allows interference of their federal governments in the production of yearly reports before their Parliaments except the Indian Personal Data Protection Bill 2019, which also provides for production of the report before Parliament by the Central government without delay unlike the draft Personal Data Protection Bill 2020 which provides a three (3) months time period to the federal government to present yearly report before the Parliament.

3. Rights of Data Subjects / Responsibilities of Data Controllers & Processors

3.1. *Obligation to Notify Data Subject*

Section 6 of the draft Personal Data Protection Bill 2020 deals with notice to the "data subject" where its data is being processed. This is provided in Article 13 and 14 of the GDPR. Section 7 of the Indian Personal Data Protection Bill 2019 provides a list of information that the data fiduciary has to provide to the data principal when collecting their data regardless of whether the data is collected from the data principal or someone else.

3.2. *Data Subject's Right to Access Processed Personal Data*

The draft Personal Data Protection Bill 2020 provides no information as to what should be provided to the "data subject" in response to their request to access data. Other jurisdictions provide lists of information that need to be provided to the "data subject".

Section 16.1 of the draft Personal Data Protection Bill 2020 entails that a "data subject" can access personal data processed by a "data controller". Same rights are provided under the DPA 2018 and Article 15 of the GDPR.

Circumstances laid down in Section 18 of the draft Personal Data Protection Bill 2020 where a "data controller" may refuse to comply with data access requests seem unjustified. The Section has been copied from the Malaysian Personal Data Protection Act 2010.

Section 17 of the Indian Personal Data Protection Bill 2019 deals with data principal's right to confirmation and access to the processed personal data. The data principal has the right to obtain from the data fiduciary confirmation whether the data fiduciary is processing or has processed personal data of the data principal, the personal data of the data principal being processed or that has been processed by the data fiduciary, or any summary thereof and a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal, including any information provided in the notice for collection or processing of personal data in relation to such processing. The data principal shall have the right to access in one place the identities of the data fiduciaries with whom their personal data has been shared by any data fiduciary together with the categories of personal data shared with them, in such manner as may be specified by regulations that are yet to be promulgated. These rights have not been dealt with in the draft Personal Data Protection Bill 2020.

3.3. *Right to Apply for Correction & Erasure*

Under Section 19 of the draft Personal Data Protection Bill 2020, a "data subject" has a right to apply for correction of their personal data held and processed by a "data controller". However, under Section 21, the "data controller" may refuse to comply with the correction request if the "data controller" is not sure the data being provided is accurate. Rectification of data processed by law enforcement is dealt by the DPA 2018 in Sections 46, 47, and 48 whereby the "data controller" is required to inform the "data subject" if the request has been granted or refused. In dealing with transfer of data processed by intelligence services under Section 100, data can only be rectified or erased.

Under Section 18 of the Indian Personal Data Protection Bill 2019, the data principal has, subject to such conditions and in such manner as may be specified by regulations, the right to the correction of inaccurate or misleading personal data, the completion of incomplete personal data, the updating of personal data that is out-of-date; and the erasure of personal data which is no longer necessary for the purpose for which it was processed. Under Section 20 the data principal shall have the right to restrict or prevent the continuing disclosure of their personal data by a data fiduciary where such disclosure has served the purpose for which it was collected or is no longer necessary for the purpose, or was made with the consent of the data principal under section 11 and such consent has since been withdrawn; or was made contrary to the provisions of this Act or any other law for the time being in force.

Article 19 of GDPR and Section 48 of the DPA 2018 also require the "data controllers" to notify the "data subject" about the erasure of data.

3.4. *Right to Make Complaints*

Section 45 of the draft Personal Data Protection Bill 2020 deals with the "data subject's" right to make complaints. Any individual may file a complaint before the Authority against any violation

of personal data protection rights, conduct of any "data controller", "data processor" or their processes. The Authority will have to acknowledge the receipt of complaint within three working days and dispose of the complaint under intimation to the complainant within thirty days of its receipt. This time period can be extended for as long as the Authority requires. The Authority will have the right to issue directions to stop breach of data protection rights of a "data subject" without first seeking comments from the concerned "data processor" and "data controller". Under Section 46, a "data subject" will be able to appeal the orders of the Authority to the High Court or to any other Tribunal established by the Federal Government and the Court or the Tribunal shall decide such appeal within ninety days.

Section 93 of the Malaysian Personal Data Protection Act 2010 provides the right to make complaints to whoever is aggrieved by the decision of the Commissioner and to appeal to the Appeal Tribunal established under Section 83.

Section 165 of the UK DPA 2018 confers upon "data subjects" the right to make complaints. The same right is provided to a "data subject" in GDPR under Article 77. Section 32 of the Indian Personal Data Protection Bill 2019 provides mechanism for grievance redressal by data fiduciary also providing right to file complaint with the Authority in case the data fiduciary is unable to solve the complaint. Section 64 provides fines as compensation for the offences.

4. Liabilities of Data Controllers & Processors

Chapter VII of the draft Personal Data Protection Bill 2020 deals with complaints and offences under the law. Section 41 of the bill deals with unlawful processing of data and imposes fines in cases of unlawful processing. Section 42 imposes fines in case of failure to adopt appropriate data security measures. Failure to comply with the orders of the Authority or a court leads to fines as well. These sections however do not merit liability.

Chapter X of the Indian Personal Data Protection Bill 2019 deals with penalties and compensation. Section 57 provides that for some offences the maximum penalty shall not exceed five crore rupees while for others it cannot exceed fifteen crore rupees.

Under Section 105 of the Malaysian Personal Data Protection Act 2010, a Commissioner is empowered to carry out an investigation in relation to the relevant data user to ascertain whether the act, practice or request specified in the complaint contravenes the provisions of the Act. As per Section 135, a Sessions Court has jurisdiction to try any offence under this Act and to impose full punishment for any such offence under this Act. Under Section 134, no prosecution for an offence under this Act shall be instituted except by or with the written consent of the Public Prosecutor. Section 132 states that all offences under this Act are compoundable.

Under the UK DPA 2018, as per Section 197, proceedings for an offence under the UK DPA 2018 may be instituted only by the Commissioner, or by or with the consent of the Director of Public Prosecutions in England and Wales. In Northern Ireland, proceedings may be instituted only by the Commissioner, or by or with the consent of the Director of Public Prosecutions for Northern Ireland. Section 198 deals with liability of directors etc and provides that where an offence under this Act has been committed by a body corporate, and it is proved to have been committed with the consent or connivance of or to be attributable to neglect on the part of a director, manager, secretary or similar officer of the body corporate, or a person who was purporting to act in such a capacity, the director, manager, secretary, officer or person, as well as the body corporate, is guilty of the offence and liable to be proceeded against and punished accordingly. Where the affairs of a body corporate are managed by its members, the law applies in relation to the acts and omissions of a member in connection with the member's management functions in relation to the body as if the member were a director of the body corporate. The Act provides fines as penalties for violations of the provisions of the Act.

Chapter 8 of the GDPR provides each natural or legal person the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them and have a

right to an effective judicial remedy where their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation, without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation has the right to receive compensation from the "controller" or "processor" for the damage suffered. This chapter lays down conditions for fines as well.

5. Procedures under the Laws

In the the draft Personal Data Protection Bill 2020, under Section 6, the “data controller” is bound to inform the “data subject” that the personal data of the “data subject” is being collected by or on behalf of a “data controller”, and shall provide:

1. a description of the personal data to that “data subject”,
2. the legal basis for the processing of personal data and time duration for which data is likely to be processed and retained thereafter,
3. the purposes for which the personal data is being or is to be collected and further processed,
4. any information available to the “data controller” as to the source of that personal data,
5. information on the “data subject’s” right to request access to and to request correction of the personal data and how to contact the “data controller” with any inquiries or complaints in respect of the personal data,
6. information on the class of third parties to whom the “data controller” discloses or may disclose the personal data,
7. information on the choices and means the “data controller” offers the “data subject” for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data, whether it is obligatory or voluntary for the “data subject” to supply the personal data, where it is obligatory for the “data subject”

to supply the personal data and the consequences for the "data subject" if he fails to supply the personal data.

Section 7 of the Indian Personal Data Protection Bill 2019 provides a list of information that the data fiduciary has to provide to the data principal when collecting their data regardless of whether the data is collected from the data principal or someone else. The list includes:

1. the purposes for which the personal data is to be processed;
2. the nature and categories of personal data being collected;
3. the identity and contact details of the data fiduciary and the contact details of the data protection officer;
4. the right of the data principal to withdraw his consent, and the procedure for such withdrawal (if the personal data is intended to be processed on the basis of consent);
5. the basis for such processing; and
6. the consequences of the failure to provide such personal data (if the processing of the personal data is based on the grounds other than consent);
7. the source of such collection (if the personal data is not collected from the data principal);
8. the individuals or entities including other "data fiduciaries" or "data processors", with whom such personal data may be shared;
9. the information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out;
10. the period for which the personal data shall be retained in terms of section 9 or where such period is not known, the criteria for determining such period;
11. the existence of and procedure for the exercise of rights mentioned in Chapter V and any related contact details for the same;
12. the procedure for grievance redressal;
13. the existence of a right to file complaints to the Authority;
14. any rating in the form of a data trust score that may be assigned to the data fiduciary; and
15. any other information as may be specified by the regulations.

The provisions shall not apply where such notice substantially prejudices the purpose of

processing of personal data without consent in certain cases.

Whereas according to Article 13 of GDPR, the “data controller” must also provide, where applicable,

1. the identity and the contact details of the "controller" and the “controller’s” representative,
2. the contact details of the data protection officer,
3. the legitimate interests pursued by the "controller" or by a third party, the recipients or categories of recipients of the personal data,
4. the fact that the "controller" intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission,
5. reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available,
6. the existence of the right to request from the "controller" access to and rectification or erasure of personal data or restriction of processing concerning the “data subject” or to object to processing as well as the right to data portability,
7. the existence of the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal,
8. the right to lodge a complaint with a supervisory authority,
9. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract,
10. the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the “data subject”.
11. Where the "controller" intends to further process the personal data for a purpose other than that for which the personal data were collected, the "controller" shall prior to that further processing provide the “data subject” with information on the other purpose and with any further relevant information.

Under Article 14 of GDPR, where the information is obtained from someone else, the "data controller", along with some of the information mentioned above, must also provide:

1. the categories of personal data concerned,
2. the source from where the personal data originated, and
3. if applicable, whether it came from publicly accessible sources.

Section 7 of the Malaysian Personal Data Protection Act under its "Notice and Choice Principle" provides a list of information to be provided to the "data subject".

1. that personal data of the "data subject" is being processed by or on behalf of the data user, and shall provide a description of the personal data to that "data subject";
2. the purposes for which the personal data is being or is to be collected and further processed;
3. of any information available to the data user as to the source of that personal data;
4. of the "data subject's" right to request access to and to request correction of the personal data and how to contact the data user with any inquiries or complaints in respect of the personal data;
5. of the class of third parties to whom the data user discloses or may disclose the personal data;
6. of the choices and means the data user offers the "data subject" for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;
7. whether it is obligatory or voluntary for the "data subject" to supply the personal data; and
8. where it is obligatory for the "data subject" to supply the personal data, the consequences for the "data subject" if he fails to supply the personal data.

From the above comparison it can be concluded that the information that the "data controller" is bound to provide to the "data subject" under the draft Personal Data Protection Bill 2020 must

also at least include:

6. the information regarding any cross-border transfer of the personal data that the "data controller" intends to carry out,
7. where the period for which the personal data will be retained is not known, the criteria for determining such period,
8. whether the data came from publicly accessible sources,
9. the procedure for grievance redressal,
10. the existence of a right to file complaints to the Authority,
11. all other rights of the "data subject".

11.1. *Cross-border Transfers*

Regarding cross-border transfer of personal data, under Section 15 of the draft Personal Data Protection Bill 2020, the decision has been left open to the discretion of the Authority.

Under the DPA 2018, the transfer of data processed by the law enforcement is dealt in Part 3, Chapter 5 where detailed framework is given by the Act itself. The Act provides general principles for transfers, separate procedures for transfers on the basis of adequacy decision and on the basis of appropriate safeguards. Transfers on the basis of special circumstances and transfers to persons other than relevant authorities have been dealt with differently. There are also separate protocols to ensure transferred data remains protected and is not further transferred. Further, transfer of data processed by intelligence services in the DPA 2018 is dealt with in Part 4, Chapter 5. Transfer of the data is prohibited unless for the purposes of the "controller's" statutory functions, or for other purposes provided for, in relation to the "controller", in section 2(2)(a) of the Security Service Act 1989 or section 2(2)(a) or 4(2)(a) of the Intelligence Services Act 1994.

Chapter VII of the Indian Personal Data Protection Bill 2019 deals with transfer of personal data outside India. Section 33 states that the sensitive personal data may be transferred outside India

on some conditions, but such sensitive personal data shall continue to be stored in India. However, the critical personal data (personal data to be notified by the Central Government) can only be processed in India except where such transfer is to a person or entity engaged in the provision of health services or emergency services where such transfer is necessary for prompt action required to take to legally process data under the bill (any such transfer is supposed to be notified to the Authority within such period as may be specified by regulations), or to a country or, any entity or class of entity in a country or, to an international organisation, where the Central Government has deemed such transfer to be permissible under clause and where such transfer in the opinion of the Central Government does not prejudicially affect the security and "strategic interest" of the State.

The conditions on which personal data may be transferred outside India are when explicit consent is given and the transfer is made pursuant to a contract or intra-group scheme approved by the Authority after some conditions laid down in the bill, and the Central Government, after consultation with the Authority, has allowed the transfer to a country or, such entity or class of entity in a country or, an international organisation on the basis of its finding that such sensitive personal data shall be subject to an adequate level of protection whereas such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction, provided that any finding under this clause shall be reviewed periodically in such manner as may be prescribed, and the Authority has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose.

Under Section 129 of the Malaysian Personal Data Protection Act 2010, the transfer of personal data to places outside Malaysia is prohibited unless to such place as specified by the Minister, upon the recommendation of the Commissioner. For these purposes, the Minister may specify any place outside Malaysia if

1. there is in that place in force any law which is substantially similar to this Act, or that serves the same purposes as this Act; or
2. that place ensures an adequate level of protection in relation to the processing of personal

data which is at least equivalent to the level of protection afforded by this Act.

3. A data user may also transfer any personal data to a place outside Malaysia if the "data subject" has given his consent to the transfer or if the transfer is necessary for the performance of a contract between the "data subject" and the data user or the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which is entered into at the request of the "data subject"; or
4. it is in the interests of the "data subject" or the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights or the data user has reasonable grounds for believing that in all circumstances of the case or the transfer is for the avoidance or mitigation of adverse action against the "data subject"; or
5. it is not practicable to obtain the consent in writing of the "data subject" to that transfer; and or if it was practicable to obtain such consent, the "data subject" would have given his consent; or the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of this Act or the transfer is necessary in order to protect the "vital interests" of the "data subject"; or the transfer is necessary as being in the public interest in circumstances as determined by the Minister.

The GDPR also provides general principles for transfers, separate procedures for transfers on the basis of adequacy decisions and on the basis of appropriate safeguards. Therefore, provisions for a detailed framework for cross-border transfer of personal data in the draft Personal Data Protection Act 2020 should be considered instead of leaving it open to the discretion of the Authority.

11.2. *Right of data subject to access personal data*

Section 16.1 of the draft Personal Data Protection Bill 2020 that deals with a "data subject's"

right to access personal data processed by a "data controller", provides no information as to what should be provided to the "data subject".

The DPA 2018 instead, lists the information that should be provided to the "data subject" in Section 45, 94 and 95 of the Act. The information listed down under Section 45 is:

1. the purposes of and legal basis for the processing;
2. the categories of personal data concerned;
3. the recipients or categories of recipients to whom the personal data has been disclosed (including recipients or categories of recipients in third countries or international organisations);
4. the period for which it is envisaged that the personal data will be stored or, where that is not possible, the criteria used to determine that period;
5. the existence of the "data subject's" rights to request from the "controller", i) rectification of personal data, and ii) erasure of personal data or the restriction of its processing;
6. the existence of the "data subject's" right to lodge a complaint with the Commissioner and the contact details of the Commissioner;
7. communication of the personal data undergoing processing and of any available information as to its origin.

The "controller" is authorized to restrict, wholly or partly, the abovementioned rights conferred to the extent that and for so long as the restriction is, having regard to the fundamental rights and "legitimate interests" of the "data subject", a necessary and proportionate measure to avoid obstructing an official or legal inquiry, investigation or procedure; or to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; or to protect public security; or to protect national security; or to protect the rights and freedoms of others. Where the rights of access of a "data subject" are restricted, wholly or partly, the "controller" is obligated to inform the "data subject" in writing without undue delay to the extent that the provision of the information would not undermine the purpose of the restriction:

1. that the rights of the "data subject" have been restricted,
2. of the reasons for the restriction,
3. of the "data subject's" right to make a request to the Commissioner,
4. of the "data subject's" right to lodge a complaint with the Commissioner, and
5. of the "data subject's" right to apply to a court.

The "controller" is also obligated to record the reasons for a decision to restrict (whether wholly or partly) the rights of a "data subject" and if requested to do so by the Commissioner, make the record available to the Commissioner.

Article 15 of the GDPR also lists the information that should be provided to the "data subject" in response to the request for access. The "data subject" has the right to obtain from the "controller" confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

1. the purposes of the processing;
2. the categories of personal data concerned;
3. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
4. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
5. the existence of the right to request from the "controller" rectification or erasure of personal data or restriction of processing;
6. of personal data concerning the "data subject" or to object to such processing;the right to lodge a complaint with a supervisory authority;
7. where the personal data are not collected from the "data subject", any available information as to their source;
8. the existence of automated decision-making, including profiling, and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the "data subject".

Under the GDPR, where personal data are transferred to a third country or to an international organisation, the "data subject" has the right to be informed of the appropriate safeguards relating to the transfer.

11.3. *Time limits*

Under Section 6.2 of the draft Personal Data Protection Bill 2020, the notice for processing of personal data shall be given as soon as reasonably possible by the "data controller". Time period for response to the request in the draft Personal Data Protection Bill 2020 with regards to compliance with data access requests is thirty (30) days.

The Data fiduciary in the Indian Personal Data Protection Act 2019 is not bound by time limit for notifying the data principle. Data fiduciary is supposed to give notice under section 7 "as soon as reasonably practicable". According to Section 21(3) of the Indian Personal Data Protection Bill 2019, the data fiduciary can comply and communicate the compliance with the request for confirmation and access, request to correct and erase data and requests under right to be forgotten, within period as specified by regulations.

Under Section 7 (2) of the Malaysian Personal Data Protection Act 2010, the notice for processing of personal data is given as soon as practicable by the data user. Under Section 31, compliance requests have to be responded to within twenty-one (21) days.

The DPA 2018 provides details about the applicable time period in Section 54 providing a time period of one (1) month and not more than three (3) months. The GDPR also provides under Article 12 an applicable time period of one (1) month to comply with requests.

From the above comparison, the time period provided in all the jurisdictions to respond to the requests does not seem ideal. For example, the time period for notifying a "data subject" for

processing of personal data is not stipulated in the Malaysian Personal Data Protection Act 2010; the notice is given as soon as reasonably possible for the "data controller". The same provision has been duplicated in India's Personal Data Protection Bill 2019 and Pakistan's draft Personal Data Protection Bill 2020. The draft Personal Data Protection Bill 2020 also provides an equal amount of time period to carry out data correction and to simply convey refusal to correct data.

11.4. *Response to Correction & Erasure Requests*

With regards to correction of personal data dealt with Section 19 of the draft Personal Data Protection Bill 2020, a "data controller" acts upon the request of the "data subject". However under Section 21, the "data controller" may refuse to comply with the correction request if the "data controller" is not sure the data being provided is accurate. In case of refusal, the "data controller" is required to inform the "data subject" of the refusal and the reasons for the same.

Rectification of data processed by law enforcement is dealt by the DPA 2018 in Sections 46, 47 and 48 whereby the "data controller" is required to inform the "data subject" if the request has been granted or refused. In case the request has been granted, the "data controller" acts on the request of the "data subject" without undue delay. In case of refusal, the "data subject" is informed of the reasons for the refusal, the "data subject's" right to make a request to the Commissioner, the data subject's right to lodge a complaint with the Commissioner, and the "data subject's" right to apply to a court. In dealing with transfer of data processed by intelligence services under Section 100, data can only be rectified or erased by the orders of the High Court in the UK except Scotland where orders of the Sessions Court suffice.

Under Section 18 (2) of the Indian Personal Data Protection Bill 2019, where the data fiduciary receives a request under Section 18 (2), and the data fiduciary does not agree with such correction, completion, updation or erasure having regard to the purposes of processing, such data fiduciary shall provide the data principal with adequate justification in writing for rejecting the application. Where the data principal is not satisfied with the justification provided by the

data fiduciary, the data principal may require that the data fiduciary take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the data principal.

As per Section 21 of the Indian Personal Data Protection Bill 2019, where any request is refused by the data fiduciary, it shall provide the data principal the reasons in writing for such refusal and shall inform the data principal regarding the right to file a complaint with the Authority against the refusal, within such period and in such manner as may be specified by regulations. The data fiduciary is not obliged to comply with any request where such compliance shall harm the rights of any other data principal under the bill.

Section 27 of the the draft Personal Data Protection Bill 2020, copied from Section 17 of the GDPR, requires erasure of data where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, the “data subject” withdraws consent on which the processing is based and where there is no other legal ground for the processing, the “data subject” objects to the processing, the personal data have been unlawfully processed or the personal data have to be erased for compliance with a legal obligation. Under the DPA 2018 under Sections 47 and 48, the “controller” has to erase personal data without undue delay where the data has been collected illegally, where there is legal obligation to erase, restrict processing where data required for to be maintained for the purposes of evidence. There are further provisions for restriction of processing of data under the same sections. For example, when the personal data must be maintained for the purposes of evidence, the "controller", required to erase personal data, must instead of erasing the personal data restrict its processing. Where a “data subject” contests the accuracy of personal data, but it is not possible to ascertain whether it is accurate or not, the "controller" must restrict its processing.

Section 9 of the Indian Personal Data Protection Bill 2019, deals with data erasure where the purpose for which data was retained has been satisfied. The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing unless explicitly consented to by the

data principal, or necessary to comply with any obligation under any law for the time being in force. Such data shall be deleted in such manner as may be specified by regulations. The data fiduciary shall undertake periodic review to determine whether it is necessary to retain the personal data in its possession. Under Section 20, the data principal shall have the right to restrict or prevent the continuing disclosure of their personal data by a data fiduciary where such disclosure:

1. has served the purpose for which it was collected or is no longer necessary for the purpose, or
2. was made with the consent of the data principal under section 11 and such consent has since been withdrawn; or
3. was made contrary to the provisions of this Act or any other law for the time being in force.

Like the Indian Personal Data Protection Bill 2019, it is recommended that where the "data subject" is not satisfied with the justification provided by the "data controller" for refusal of the correction/completion.updation/erasure request, the "data subject" be provided the right to require that the "data controller" to restrict processing or take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the "data subject".