PERSONAL DATA PROTECTION ACT

MICROFINANCE & LENDING INSTITUTIONS

FJ&G de Saram
Attorneys-at-law

THE PDPA – WHAT IS IT AND HOW DID IT COME ABOUT?

In 2019, the Ministry of Digital Infrastructure and Information Technology introduced the Personal Data Protection Bill (the "PDPB") for *inter alia* the regulation of processing of personal data.

The PDPB is inspired by the General Data Protection Regulation ("GDPR") of the European Economic Area.

Personal Data Protection Act No. 9 of 2022 ("PDPA") was passed by the Parliament on the 19th of March 2022.

FJ&G de Saram
Attorneys-at-law

WHAT DOES THE PDPA DO?

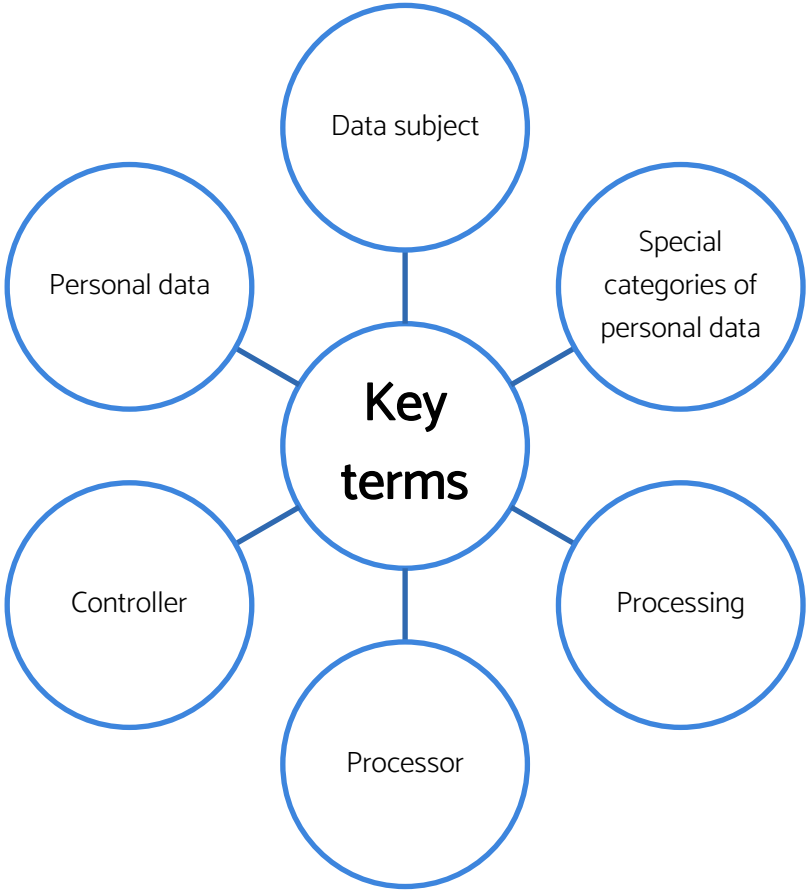
Grants rights to data subjects

Imposes obligations on entities that process personal data

Regulates direct marketing

Provides for enforcement authority

Imposes severe penalties for violations


Data subject
Personal data
Special categories of personal data
Key terms
Controller
Processing
Processor

PERSONAL DATA

Any information that can **identify a data subject** directly or indirectly either by reference to an indicator or by one or more factors specific to the data subject

DATA SUBJECT

A **natural person**, alive or deceased, to whom the personal data relates

SPECIAL CATEGORIES OF PERSONAL DATA

personal data including:

- racial or ethnic origin
- political opinions
- religious and philosophical beliefs
- biometric data
- genetic data
- health data
- Offences, criminal proceedings and convictions
- sex life & sexual orientation
- data relating to a child

PROCESSING

Any operation performed on personal data:
Collection, storage, preservation, alteration, retrieval, disclosure, transmission, making available, erasure, destruction of, consultation, alignment. combination, or the carrying out of logical or arithmetical operations on personal data.

CONTROLLER

- Determines the **purposes** of processing personal data
- Determines the **means** of processing personal data

PROCESSOR

Processes personal data
on behalf of controller

PROCESSOR V PROCESSING

Important to note the difference between ‘processor’ and ‘processing’.

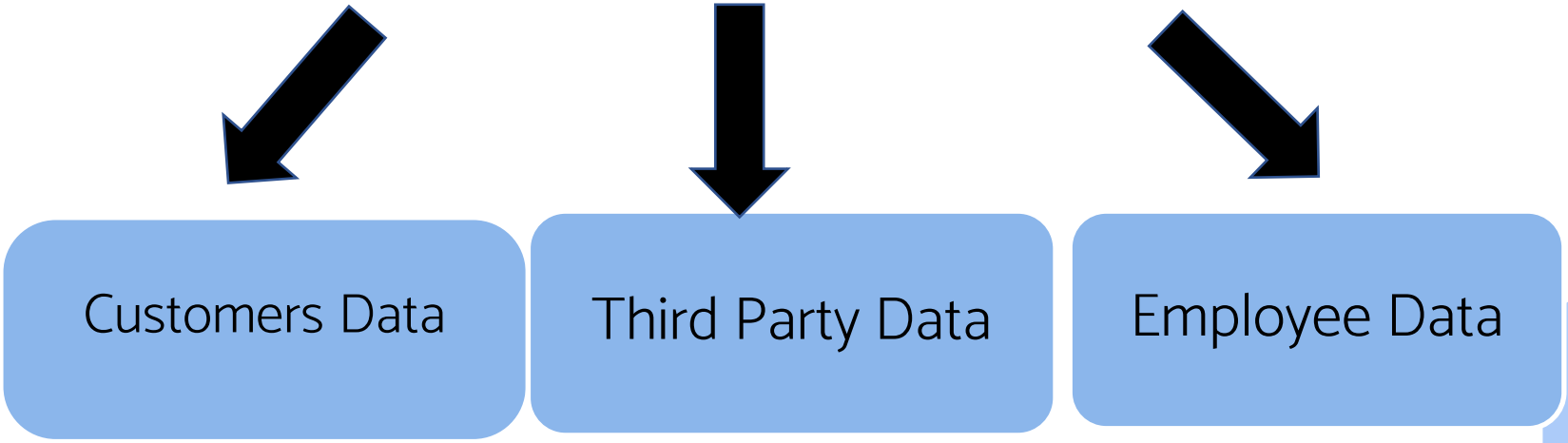
Processors and controllers both partake in processing

A controller will not always need a processor.

APPLICABILITY OF PDPA

1) Process personal data wholly or partly within Sri Lanka; or
2) The entity is resident in Sri Lanka; or
3) Registered or incorporated or established under the Companies Act; or
4) Offers goods or services to data subjects in Sri Lanka; or
5) Monitors behavior of data subjects.

WHAT TYPE OF PERSONAL DATA MAYBE COLLECTED?



CONSUMER DATA

FJ&G de Saram
Attorneys-at-law

DOES THE PDPA APPLY TO EXISTING PERSONAL DATA?

Yes

ARE YOU THE CONTROLLER OR THE PROCESSOR?

FJ&G de Saram
Attorneys-at-law

Depends on the activities that you have undertaken

CONTROLLER	PROCESSOR
Granting of microfinance loans and credit facilities	
Deposits account creation (if licensed)	
Providing skills and knowledge to start and operate micro and small business ventures	
Marketing/promotional activities targeting end consumer	
Training programmes	
Automated decision/profiling	
Monitoring customers payment behaviors	
Collection of information of the employees	
Collecting and sharing credit and financial information on borrowers of the Microfinance companies	

WHAT IS EXPECTED OF YOU AS A CONTROLLER?

FJ&G de Saram
Attorneys-at-law

Identify the purpose → Ascertain whether the purpose has a lawful basis → Confine to the purpose/minimization

WHAT ARE THE DIFFERENT PURPOSES FOR PROCESSING DATA

FJ&G de Saram
Attorneys-at-law

BUSINESS FUNCTION	PURPOSE OF PROCESSING
Grant of credit facilities and deposit taking	Monitoring customers payment behaviors
	Collection of repayments
	Customer profiling
Human Resources	Personnel File
	Recruitment
	Payroll

WHAT ARE THE LAWFUL GROUNDS FOR PROCESSING PERSONAL DATA?

FJ&G de Saram
Attorneys-at-law

- **Necessary** for performance of **a contract**/to enter into a contract with a data subject ; or
- **Necessary** for compliance with **a legal obligation** to which controller is subject to under any written law ; or
- **Necessary** for purposes of **legitimate interests** pursued by the controller or by a third party; or
- Consent.

LAWFUL GROUNDS- Cont'd

NECESSARY FOR PERFORMANCE OF A CONTRACT/TO ENTER INTO A CONTRACT WITH A DATA SUBJECT

Loan facility

Deposit taking (if licensed)

NECESSARY FOR LEGITIMATE INTEREST PURSUED BY THE CONTROLLER OR BY A THIRD PARTY

Prevention of fraud

Network and information security

LAWFUL GROUNDS- Cont'd

FJ&G de Saram
Attorneys-at-law

NECESSARY FOR COMPLIANCE WITH A LEGAL OBLIGATION TO WHICH A CONTROLLER IS SUBJECT TO UNDER ANY LAW

Direction No. 07 of 2016 (Regulatory Framework for Accommodation)

Assessment of fitness and propriety of directors, CEO and general manager

EPF/ETF and social security obligations and the obligations under the Shop & Office (Regulation of Employment and Remuneration) Act

CONSENT

Promotional and marketing activities

Customer preferences tracking

FOR SPECIAL DATA – ADDITIONAL CONDITIONS

FJ&G de Saram
Attorneys-at-law

- If the data is **necessary**
  - For any purpose provided for in any written law or public interest and shall be necessary and proportionate to the aim;
  - Whilst providing suitable and specific measures to safeguard the rights and freedoms of the data subject
  - Or
- If data is **necessary**
  - For establishment, exercise or defence of legal claim before a court or tribunal
  - Or such similar forum or whenever courts are acting in their judicial capacity

or

- consent

HOW DO YOU OBTAIN CONSENT?

*Consent: **any freely** given, specific, informed and unambiguous indication by way of a written declaration or affirmative action signifying a data subject's agreement to the processing of his data*

written consent:

- Clear distinguishable from other matters
- Intelligible and easily accessible form
- Using clear and plain language

Clear affirmative action

- By voice, conduct or otherwise

It is mandatory to retain records of consent

CONSENT - FREELY GIVEN

when assessing whether consent is freely given, utmost account shall be taken on whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract

WHAT OTHER OBLIGATIONS DO YOU HAVE FOR THE DATA THAT YOU COLLECT?

FJ&G de Saram
Attorneys-at-law

accuracy and completeness
integrity and confidentiality
defined retention time period
transparency
internal controls and procedures
honour the rights of the subscribers

ACCURACY AND COMPLETENESS

Data is:

- Accurate
- Kept up to date

Inaccurate or outdated data is erased or rectified

INTEGRITY AND CONFIDENTIALITY

Have appropriate organizational and technical measures to prevent:

unauthorized or unlawful processing of personal data; or

loss, destruction or damage of personal data.

DEFINED RETENTION TIME PERIOD

Documents should be retained only for period as required for the necessary purpose

However, you may need to retain for:

- evidential purposes
- Legal obligations

The privacy notice should reflect the period of retention

TRANSPARENCY

Providing mandatory information to the data subject at the point of collection

Responding to request of the data subject

MANDATORY INFORMATION TO BE PROVIDED:

FJ&G de Saram
Attorneys-at-law

Identity and contact details of the controller
Contact details of data protection officer (if applicable)
Intended purpose for collecting the data
the ability for the data subject to withdraw consent (for consent based processing)
Recipients/third parties with whom personal data may be shared
Information regarding any cross border flow
Period of retention
Existence of and procedure for the exercising of rights of the data subjects
Ability for the data subject to file a complaint with the Data Protection Authority
If obtaining personal data is a statutory/contractual requirement and consequences of not providing the information
Decisions based on automated processing
Information on the disclosures to regulatory authorities

INTERNAL CONTROLS AND PROCEDURES

FJ&G de Saram
Attorneys-at-law

Designed on the basis of structure, scale, volume, sensitivity of processing

Maintain duly catalogued records

Provides appropriate safeguards based on impact assessments

Integrated into the governance structure

Data Protection Management Programme

Establishes internal oversight

A mechanism to receive complaints, conduct inquiries, identify breaches

Updated based on periodic monitoring and assessments

HONOUR THE RIGHTS OF THE DATA SUBJECT

Access

Withdrawal of consent

Rectification or completion

Erasure

Review of automated decisions

WHAT IS RIGHT OF ACCESS?

Access to personal data

Confirmation that personal data has been processed

To obtain mandatory information required to be shared with the data subject

WHAT IS THE RIGHT TO WITHDRAW CONSENT?

Right to withdraw consent at any time

Withdrawal does not affect any processing done prior to withdrawal

WHAT IS THE RIGHT OF RECTIFICATION OR COMPLETION?

Right to request rectification

Completion of data

WHAT IS THE RIGHT TO ERASURE?

Circumstances where erasure is required:

- Processing is in violation of parameters set out under the PDPA
- Consent has been withdrawn
- Mandatory legal requirement

REVIEW OF AUTOMATED DECISIONS

FJ&G de Saram
Attorneys-at-law

Decisions based solely on automated processing

likely to create an irreversible and continuous impact on the rights and freedoms of the data subject under any written law

Not applicable if:

- permitted by any written law
- authorised by the Authority
- consumer consented
- necessary for entering into or perform contract with consumer (not for special data)

HOW CAN THE RIGHTS BE EXERCISED?

FJ&G de Saram
Attorneys-at-law

Sending a written request

WHAT DO YOU DO ON RECEIPT OF WRITTEN REQUEST?

Accede to the request; or

Refuse the request

- Unable to establish identity of the data subject
- Mandatory legal requirements
- Technical and operational feasibility to act on such request

Written reply to the the data subject, within 21 days (transparency)

Right of appeal to Data Protection Authority

THIRD PARTY DATA

THIRD PARTY DATA – CONTROLLER OR PROCESSOR?

Third party service providers

MICROFINANCE/LENDING INSTITUTION IS A CONTROLLER

THIRD PARTY SERVICE PROVIDERS

DO YOU RETAIN THIRD PARTIES TO PROCESS PERSONAL DATA?

Cloud service providers

Data analytics service providers

Processors

WHAT ARE YOUR OBLIGATIONS IN RETAINING PROCESSORS?

Assess the processor

Provide processors with a clear written contract with measures, provisions and obligations to enforce your obligations

Practical measures

Indemnity

Insurance

OTHER IMPORTANT ASPECTS

WHAT OTHER ASPECTS REQUIRE ATTENTION?

Data Protection Impact Assessment

Data Protection Officer

Retaining third parties to process personal data

Cross border transfer of data

Direct Marketing

WHAT IS A DATA PROTECTION IMPACT ASSESSMENT?

To assess impact of processing under certain circumstances

Reporting to the Data Protection Authority

Adopting the recommendations of the Data Protection Authority

Taking mitigatory steps to avoid the risk of harm

Reassessment in change of circumstances

WHEN DO YOU NEED A DATA PROTECTION IMPACT ASSESSMENT?

where you carry out:

- systematic and extensive evaluation of personal data or special categories of data including profiling
- systematic monitoring of publicly accessible areas
- Any activity prescribed by the law

Profiling: processing personal data to evaluate, analyse, predict aspects concerning data subject's performance at work, **economic situation**, health, personal preferences, interests, **credibility**, **behaviour habits**, location or movements, etc.

Publicly accessible areas: any place open to any member of the public

WHO IS A DATA PROTECTION OFFICER AND DO YOU NEED ONE?

If the core activities include:

- Large scale monitoring of data subjects
- Large scale processing of special categories of data
- Processing which might have risk of harm to data subjects

WHAT IS A CROSS BORDER DATA FLOW?

Any data flow to a third party outside Sri Lankan territory

IS CROSS BORDER DATA FLOW ALLOWED?

Adequacy decision

Without an adequacy decision and in the absence of adequate safeguards under certain grounds:-

- Explicit consent from data subject;
- Performance of contract
- Establishment, exercise of defence of legal claims against data subject
- Public interest
- Emergency threatening life, health or safety of any person
- Permitted under any conditions prescribed under PDPA

WHAT IS DIRECT MARKETING?

Any marketing communication to customer or potential customer

HOW CAN YOU USE DIRECT MARKETING?

Only with prior written consent

Messages with consent is referred to as “solicited messages” in the PDPA

Providing a method to opt out with each message

Citing the source of the personal data

Other requisite information

Exclusion- “*any internet based advertisements to which a data subject has consented to obtain a service free of charge from the controller*”

WHAT PRACTICAL MEASURES CAN YOU TAKE WHEN ENGAGING WITH A THIRD PARTY FOR DIRECT MARKETING?

Assessment of capacity to comply with the PDPA

Written contract, incorporating the provisions of the PDPA

Indemnity

Insurance

SPECIAL CONSIDERATIONS

Implications of sharing/transferring credit standing details of customers with MFPA or CRIB-like service provider

Hosting aforesaid information outside Sri Lanka

DATA PROTECTION AUTHORITY

WHO IS THE REGULATOR?

The Data Protection Authority

WHAT ARE THE OBJECTIVES?

Objectives include:

- Regulating processing of personal data
- Safeguarding privacy of data subjects
- Providing protection for personal data used in digital transactions and communications

WHAT ARE THE POWERS OF THE DATA PROTECTION AUTHORITY?

Issue directives

Make rules

Look into complaints

Conduct inquiries

Examine people under oath

Inspect any information held by a controller or processor

enter into premises of controller or processor and inspect or seize records and carry out investigations if there are reasonable grounds to believe that processing possesses an imminent risk to data subjects

WHAT ARE THE PENALTIES FOR VIOLATIONS?

FJ&G de Saram
Attorneys-at-law

If there is a violation - a directive will be issued.

Directive may include:

To cease and refrain from engaging in such act/omission

Take action to rectify situation

Make payment to aggrieved person as compensation

If the directive is not complied with – penalties will be imposed

What can you do if you receive a penalty?

An aggrieved controller or processor may appeal to the Court of Appeal within 21 working days of receiving notice of the penalty

WHEN WILL THE LAW COME INTO OPERATION?

FJ&G de Saram
Attorneys-at-law

Although the PDPA is passed, a transitional time period is provided as follows before the same being enforced.

data protection principles, rights and obligations of the controllers and processors and rights of the data subjects) will be brought into operation in 18 to 36 months from 19th March 2022.

Use of Personal Data to Disseminate Unsolicited Messages) will be brought into operation in 24 to 48 months from 19th March 2022.

Data Protection Authority – any time before Parts I, II and III are brought into operation.

THANK YOU

FJ&G de Saram
Attorneys-at-law

Questions?

Shanaka Gunasekara
Partner
Head of Data Protection & Privacy
M: +94 77 3741097
E: shanaka.gunasekara@fjgdesaram.com