TABLE OF CONTENTS

INTRODUCTION

Personal data, which is information relating to an identified or identifiable individual, is collected and used almost everywhere and has become the oil of the twenty-first century. Personal data can be an individual's name or mobile number or location data, amongst others.

As the value of personal data grows, the risks to personal data inevitably increase. In addition, with rapid technological change and innovation, controlling personal data is becoming more and more difficult especially with data intensive online activities. A robust data protection law is therefore a must and requires sound data management practices on entities processing data, also known as 'controllers'.

The Data Protection Act 2017 is an accomplished effort of this office to sustain and strengthen the control and personal autonomy of data subjects over their personal data. It has been designed to align with the key principles found in international laws namely the EU General Data Protection Regulation.

The Data Protection Act 2017 rests on several pillars namely coherent rules, simplified procedures, coordinated actions, user involvement and stronger enforcement powers. The Act aims at:

- Modernising the existing data protection principles and key definitions such as consent and personal data;

- Introducing new concepts for better information handling such as data protection impact assessments, notification of personal data breaches and communication to data subjects, voluntary certification mechanisms and rights to object to automated individual decision-making, including profiling;

- Simplifying the complaints' mechanism and the procedures related to hearings conducted by the Data Protection Office.

This introductory guide has been issued to assist controllers and processors to implement the provisions of the Data Protection Act 2017. It highlights the key changes, challenges and actions that organisations should adopt in order to achieve compliance.

DEFINITIONS

As with any legislation, certain terms have a particular meaning. The following are some key definitions:

Personal data means any information relating to a data subject.

Data subject means an identified or identifiable individual, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Processing means an operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller means a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision-making power with respect to the processing.

Processor means a person who, or public body which, processes personal data on behalf of a controller.

Consent means any freely given specific, informed and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which he signifies his agreement to personal data relating to him being processed.

Special categories of personal data, in relation to a data subject, means personal data pertaining to –

(a) his racial or ethnic origin;
(b) his political opinion or adherence;
(c) his religious or philosophical beliefs;
(d) his membership to a trade union;
(e) his physical or mental health or condition;
(f) his sexual orientation, practices or preferences;
(g) his genetic data or biometric data uniquely identifying him;
(h) the commission or alleged commission of an offence by him;
(i) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings; or
(j) such other personal data as the Commissioner may determine to be sensitive personal data;

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information and the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual.

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Third party means a person or public body other than a data subject, a controller, a processor or a person who, under the direct authority of a controller or processor, who or which is authorised to process personal data.

PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

What you need to know on principles relating to processing of personal data (section 21 of the Data Protection Act)?

The six privacy principles form the fundamental conditions which controllers must follow when collecting, processing and managing the personal information data owned by data subjects. These principles are broadly similar to those found in Schedule 1 of the Data Protection Act 2004 but are now found under a dedicated section in the Data Protection Act 2017, and a new concept 'Data Subjects' rights has been introduced as highlighted below.

Lawfulness, fairness and transparency

Personal data of data subjects must be processed lawfully, fairly, and in a transparent manner.

Example: A competition in a newspaper does not indicate that the entrants' names and addresses may be used in direct marketing. The email addresses would be fairly and transparently processed if the competition entry form stated "Your email address may be used for direct marketing purposes. If you wish your email address to be used for direct marketing purposes, please tick this box."

Purpose limitation

Personal data must be collected for explicit, specified and legitimate purposes and not further processed in a way incompatible with those purposes.

Example: A GP discloses his patient list to his wife, who runs a travel agency, so that she can offer special holiday deals to patients needing recuperation. Disclosing the information for this purpose would be incompatible with the purposes for which it was obtained.

Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Example: A recruitment agency places workers in a variety of jobs. It sends applicants a general questionnaire, which includes specific questions about health conditions that are only relevant to particular manual occupations. It would be irrelevant and excessive to obtain such information from an individual who is applying for an office job.

Accuracy

Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Example: For example, a company that sells books to individuals online doesn't need to regularly check they have the correct information about them. However, if a company awards a pay increase to a staff member, their details and salary should be checked and updated where necessary.

Storage limitation

Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Example: An employer should review the personal data it holds about an individual when that individual leaves the organisation's employment. It will need to retain enough data to enable the organisation to deal with, say, providing references or information about the individual's pension arrangements. However, personal data that is unlikely to be needed again should be removed from the organisation's records.

Data Subjects' rights

Personal data must be processed in accordance with the rights of data subjects.

Example: Data subjects have the rights to access their personal data, object to processing of their personal data e.g. for direct marketing, have inaccurate data changed, request for specific data to be erased or restricted their processing, lodge a complaint for data breaches and also withdraw their consent for processing.

Principles relating to processing of personal data

Main Points	To do list
Controllers and processors must have legitimate grounds for collecting data which do not have a negative effect on data subjects. They must also provide full transparency about how they wish to use the data, as well as ensure data is only used in ways data subjects would legitimately expect.	Review internal policies and audit procedures and update these where necessary to ensure that these are consistent with the revised principles.
Controllers and processors must be open on their reasons for obtaining personal data and what they plan to use it for. They must only use the personal data for the purpose they originally agreed it would be used for.	Ensure that appropriate training is provided to ensure that the business is thinking about data protection issues at all levels.
Data must be adequate for the purpose it is being held. Controllers and processors must avoid holding more information than necessary.	
Reasonable steps must be taken to keep the information up to date and to change it if it is inaccurate.	
Data must be held only for the amount of time required. Data that is out of date or no longer necessary must be destroyed or deleted.	
Data must be processed while taking into account data subjects' rights.	

CONSENT

What you need to know on consent (section 24 of the Data Protection Act)?

"The controller shall bear the burden of proof for establishing a data subject's consent to the processing of his personal data for a specified purpose."

1. What is consent?

Consent is any freely given specific, informed and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which he signifies his agreement to personal data relating to him being processed.

Example: A user signs an agreement on an e-commerce website to express consent about his personal data being used for the processing of his purchases.

2. Why is consent important?

Consent is one of the lawful base for processing of personal data.

3. Why is it important to obtain consent?

Handling consent well would guarantee individuals' control, build customer trust and engagement and enhance the reputation of your operations. Relying on inappropriate or invalid consent could destroy trust, harm your reputation and might leave you exposed to substantial fines.

Any person who contravenes subsection 28(1) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 5 years.

4. What is different about consent?

The key elements of the definition of consent remain: it must be freely given, specific, informed, and there must be an indication signifying agreement.

However, the DPA 2017 is clearer that the indication must be unambiguous and involve a clear affirmative action. This definition is only the starting point for a new standard of proof for consent.

5. How has consent been catered for in the DPA 2017?

Several new provisions on consent contain more detailed requirements. There are various conditions for consent, with specific provisions on keeping records of consent and the right to withdraw consent.

In essence, there is a greater emphasis in the new DPA on individuals having clear granular choices upfront and ongoing control over their consent.

6. What are the benefits of getting consent right?

Basing your processing of customer data on DPA-compliant consent means giving individuals genuine choice and ongoing control over how you use their data, and ensuring that your organisation is transparent and accountable.

7. What are the benefits of organisations to get consent right?

Getting this right should be seen as essential to good customer service and legal compliance: it will put people at the center of the relationship and can help build customer confidence and trust. This can enhance your reputation, improve levels of engagement and encourage use of new services and products. It's one way to set yourself apart from the competition.

8. What will happen if there is no valid consent?

Handling personal data badly, including relying on invalid or inappropriate consent, can erode trust in your organisation and damage your reputation. Individuals will not want to engage with you if they think they cannot trust you with their data; you do things with it that they don't understand, want or expect; or you make it difficult for them to control how it is used or shared.

9. What is the obligation of controllers?

There is a need to review your consent mechanisms to make sure that they meet the requirements on being specific, granular, clear, prominent, opt-in, documented and easily withdrawn.

10. How to ensure that the consent (as expressed by the data subject) meet the legal requirements?

- Consent should be specific, informed and unambiguous, by setting out the purpose of the various phases of the processing.
- At the time of collection, data subjects should be informed about the right to withdraw consent at any time.
- Consent should be easy to withdraw without affecting the lawfulness of processing.
- Consent should be verifiable.

11. Are there circumstances when consent is not required?

Yes. No person shall process personal data unless:-

(a) the data subject consents to the processing for one or more specified purposes;
(b) the processing is necessary –

(i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;

(ii) for compliance with any legal obligation to which the controller is subject;

(iii) in order to protect the vital interests of the data subject or another person;

(iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(v) the performance of any task carried out by a public authority;

(vi) the exercise, by any person in the public interest, of any other functions of a public nature;

(vii) for the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or

(viii) for the purpose of historical, statistical or scientific research.

Consent

Main Points	To do list
Consent is any freely given specific, informed and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which he signifies his agreement to personal data relating to him being processed.	Unbundled: Consent requests must be separate from other terms and conditions. Consent should not be a precondition for signing up to a service unless it is necessary for that service.
Ensure that you are clear about the grounds for lawful processing relied on by your organisation and check that these grounds will still be applicable under the DPA 2017	Active opt-in: pre-ticked opt-in boxes are not valid: Use unticked, opt-in boxes or similar active opt-in methods.
Basing your processing of customer data on DPA-compliant consent means giving individuals genuine choice and ongoing control over how you use their data and ensuring your organisation is transparent and accountable.	Granular: give granular options to consent separately from different types of processing wherever appropriate.
Consent should be easy to withdraw without affecting the lawfulness of processing.	Named: name your organisation and any third parties who will be relying on consent.
	Documented: keep records to demonstrate what the individual has consented to, including what they were told, when and how they consented.

CHILDREN

What you need to know on children (section 30 of the Data Protection Act)?

"No person shall process the personal data of a child below the age of 16 years unless consent is given by the child's parent or guardian.

Where the personal data of a child below the age of 16 years is involved, a controller shall make every reasonable effort to verify that consent has been given or authorised, taking into account available technology."

1. What is new regarding children?

Children's personal data now enjoys specific protection under the DPA 2017 especially when you are collecting their personal data and using it for marketing purposes or creating personalities or user profiles.

2. What rights do children have?

Children have the same rights as adults over their personal data. They can exercise their own rights as long as they are competent to do so. Where a child is not considered to be competent, an adult with parental responsibility may exercise the child's data protection rights on their behalf.

3. Who will give consent for children?

For children under 16, you need to get consent from whoever holds parental responsibility for them. You may therefore need to verify that anyone giving their own consent in these circumstances is old enough to do so and doing so in the interests and benefits of the child.

4. What precautions should be taken regarding children?

If you process children's personal data, or think that you might, then you should consider the need to protect them from the outset and design your systems and processes with this in mind.

5. What approach should be used regarding children?

You should not usually make decisions about children based solely on automated processing if this will have a legal or similarly significant effect on them. The circumstances in which the DPA 2017 allows you to make such decisions are limited and only apply if you have suitable measures to protect the interests of the children in place.

If you profile children then you must provide them with clear information about what you are doing with their personal data. You should not exploit any lack of understanding or vulnerability.

Fairness and compliance with the data protection principles should be central to all your processing of children's personal data. It is good practice to consult with children when designing your processing.

6. What should be understood by children?

When relying on consent, you must make sure that the children understand what they are consenting to and that you do not exploit any imbalance in power in the relationship between the children and the controller. You must write clear and age-appropriate privacy notices for children. The right to have personal data erased is particularly relevant when the individual gave his consent to processing when he was a child.

7. What do you need to think about when choosing a basis for processing children's personal data?

As with adults, you need to have a lawful basis for processing children's personal data and you need to decide what that basis is before you start processing.

You can use any of the lawful bases for processing set out in the DPA 2017 when processing children's personal data.

8. What if you wish to rely upon consent as your lawful basis for processing?

If you wish to rely upon consent as your lawful basis for processing, then you need to ensure that the children can understand what they are consenting to, otherwise consent would not be 'informed' and therefore invalid.

9. What if you wish to rely upon performance of a contract?

If you wish to rely upon 'performance of a contract' as your lawful base for processing, then you must consider the children's competence to agree to the contract and to understand the implications of this processing.

10. What if you wish to rely upon legitimate interests as lawful basis for processing?

If you wish to rely upon legitimate interests as your lawful base for processing, you must balance your own (or a third party's) legitimate interests in processing the personal data against the interests and fundamental rights and freedoms of the children.

This involves a judgement as to the nature and purpose of the processing and the potential risks it poses to children. It also requires you to take appropriate measures to safeguard against those risks.

Children

Main Points	To do list
A child's personal data now merits particular protection under the DPA 2017.	Consider whether rules on children are likely to affect you.
For children under 16, you need to get consent from whoever holds parental responsibility for them.	Where services are offered directly to children, ensure notices are drafted clearly with a child's understanding in mind.
You must make reasonable efforts (using available technology) to verify that the person giving consent does, in fact, hold parental responsibility for the child.	Ensure any reliance on "legitimate interests" to justify processing children's data is backed up by a careful and documented consideration of whether a children's interests override those of your organisation.
Consent should be easy to withdraw without affecting the lawfulness of processing.	Where online services are provided to a child and consent is relied on as the basis for the lawful processing of his data, consent must be given or authorised by a person with parental responsibility for the children. This requirement applies to children under the age of 16.
As with adults, you need to have a lawful basis for processing children's personal data and you need to decide what that basis is before you start processing.	

RIGHTS OF DATA SUBJECTS

What you need to know on the rights of data subjects (sections 37 to 41 of the Data Protection Act 2017)?

"Every controller shall, on the written request of a data subject provide, at reasonable intervals, without excessive delay and, subject to subsection (7), free of charge, confirmation as to whether or not personal data relating to the data subject are being processed and forward to him a copy of the data."

1. What is different in the DPA 2017?

The rights to access, rectify, erase and restrict processing have been enhanced. New provisions have been made to cater for decisions which are based on automated processing and the right to object to the processing of personal data by data subjects.

2. What does "fair and transparent" processing means?

The principle of "fair and transparent" processing means that the controller must provide relevant information to the individual about the processing of his data, unless the individual already has this information.

3. What must a controller inform individuals about the personal data collected?

- The purpose/s for which the data are being collected;
- The intended recipients of the data;
- Whether or not the supply of the data by that data subject is voluntary or mandatory;
- The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- The existence of the right to request from the controller access to and rectification, restriction or erasure of personal data concerning the data subject or to object to the processing;
- The existence of automated decision making, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- The period for which the personal data shall be stored;
- The right to lodge a complaint with the Commissioner;
- Where applicable, that the controller intends to transfer personal data to another country and on the level of suitable protection afforded by that country; and
- Any further information necessary to guarantee fair processing in respect of the data subject's personal data, having regard to the specific circumstances in which the data are collected.

4. When must the controller provide these details about the personal data collected?

Where the controller obtains personal data directly from the individual, the latter should be informed about the details (in point 3) at the time the data are being collected.

Where the controller does not obtain personal data directly from the individual, the latter should be informed about these details (in point 3) within a reasonable period of having obtained the data.

5. What are the rights of information and access of data subjects?

An individual has the following rights:

- to obtain confirmation whether his/her personal data are being processed;
- to access the data (i.e. to a copy); and
- to be provided with supplemental information about the processing.

Access rights are intended to allow individuals to check the lawfulness of processing and the right to have a copy of their personal data. However, these rights should not adversely affect the rights of others.

6. How should the request be handled?

A written request must be provided by the data subject. The controller should provide the information, at reasonable intervals, without excessive delay and free of charge, confirmation as to whether or not personal data relating to the data subject are being processed and forward to him a copy of the data.

In case the request is manifestly excessive, the controller may charge a fee for providing the information or taking the action requested, or else the requested action will not be taken.

7. What should be done for the rights of information and access of data subjects?

The controller must also use reasonable means to verify the identity of the person making the request but should not keep or collect data just so as to be able to meet subject access requests. These points are particularly pertinent to online services.

Individuals can require a controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data are incomplete, an individual can require the controller to complete the data or to record a supplementary statement.

8. When is the controller not required to provide for the rights of information and access to data subjects?

Where the personal data are not or have not been collected from the data subject, the controller shall not be required to provide information where the processing is expressly prescribed by law or this proves to be impossible or involves a disproportionate effort.

9. What rights of rectification do data subjects have?

- Rectify inaccuracies in personal data held about them.
- Complete incomplete data
- Record a supplementary statement.

10. In what circumstances does the controller need to erase personal data of data subjects?

- The data are no longer necessary in relation to the purpose 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 of personal data and there are no overriding legitimate grounds for the processing.
- The personal data have been unlawfully processed.

11. What happens if the controller has made the data public?

The controller should inform third parties processing the personal data about the request of data subjects for the erasure of any links to, or copy or replication of, their personal data.

12. What should be done for the right to erasure and right to restriction of processing of data subjects?

- Ensure that members of staff and suppliers who may receive data erasure requests recognise them and know how to deal with them.
- Determine if you work in a sector where compliance with erasure requirements would be so unreasonable that exemptions should be sought.
- Determine if systems are able to meet the requirements to mark data as restricted whilst complaints are resolved: undertake development work if needed.

13. When should the controller not comply to the request for rectification and erasure?

- For reasons of public interest in the field of public health
- For the purpose of historical, statistical or scientific research
- For compliance with a legal obligation to process the personal data to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- For the establishment, exercise or defence of a legal claim.

14. When should the controller restrict processing following the request of data subjects?

- The accuracy of the personal data is contested by the data subject and processing should be restricted for the period during which the controller can verify the accuracy of the data.
- The controller no longer needs the personal data for processing but the data subject requires them for the establishment, exercise or defence of a legal claim.
- The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead.
- The data subject has objected to the processing pursuant to section 41 pending verification as to whether the legitimate grounds of the controller override those of the data subject.

15. How should the processing of restricted personal data be handled?

Except for storage purposes, the personal data should only be processed with the data subject's consent or for the establishment, exercise or defence of a legal claim, the protection of the rights of another person or for reasons of public interest. The controller should inform the data subject before lifting the restriction on processing of the personal data.

According to section 39 (7), the controller shall implement mechanisms to ensure that the time limits established for the rectification, erasure or restriction of processing of personal data, or for a periodic review of the need for the storage of the personal data, are observed.

16. What are the rights to object of data subjects?

The data subject has the right to object in writing at any time to the processing of personal data concerning him.

The data subject has to the right to object to direct marketing which includes profiling.

17. What is profiling?

Profiling is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict certain aspects concerning that person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

18. When are the restrictions concerning decisions taken regarding individuals through automated processing waived?

Subject to section 38 (1), every data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or significantly affects him unless it is:

- necessary for entering into, or performing, a contract between the data subject and a controller
- authorised by a law to which the controller is subject to and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or
- based on the data subject's explicit consent.

Any automated processing of personal data intended to evaluate certain personal aspects relating to an individual should not be based on special categories of personal data.

Furthermore, the information to be provided by the controller under section 23 (collection of personal data) should include information as to the existence of processing for a decision of the kind referred to subsection in 38 (1) and the envisaged effects of such processing on the data subject.

In addition, the controller should implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

19. To whom are the rights to individuals conferred to?

- Where the data subject is a minor, by a person who has parental authority over the child or has been appointed as his guardian
- Where the data subject is physically or mentally unfit, by a person who has been appointed as his guardian or legal administrator by a Court; or
- In any other case, by a person duly authorised in writing by the data subject to make a request.

20. What are the obligations of Controllers?

Action	Timing
1. To comply with request for information and access	Inform data subjects without undue delay and at latest within one month. Period may be extended by a further month where necessary, taking into account the complexity and the number of requests made.
2. When request is received	Inform data subjects within 1 month of request whether actions have been taken or not.
3. Where a controller refuses to take action on the request of a data.	Inform data subjects of the reason/s for the refusal and on the possibility of lodging a complaint with the Commissioner within one month.
4. When a request for rectification, erasure or restriction of processing is received.	Without undue delay

Rights of Data Subjects

Main Points	To do list
Controllers must, on request: • confirm if they process an individual's personal data • provide a copy of the data • provide supporting explanatory materials.	Controllers must provide information notices to ensure transparency of processing.
Access rights are intended to allow individuals to check the lawfulness of processing and the right to have a copy of their personal data. However, the rights should not adversely affect the rights of others.	Use reasonable means to verify the identity of the person making the request.
	Consider developing data subjects access portals, to allow direct exercise of subject access rights.
Data subjects have the rights to rectification, erasure and restriction of processing of their personal data.	Take the required action without undue delay and inform the data subjects accordingly.
Data subjects have the rights for individuals to object to the processing of personal data like direct marketing which includes profiling.	Ensure that members of staff and suppliers who may receive data erasure requests recognise them and know how to deal with them. Determine if you work in a sector where compliance with erasure requirements would be so unreasonable that exemptions should be sought. Determine if systems are able to meet the requirements to mark data as restricted to find a solution if it is not the case.
	Audit data protection notices and policies are required to ensure that individuals are told about their right to object, clearly and separately, at the point of 'first communication'. For online services, ensure there is an automated way for this to be effected; Review marketing suppression lists and processes (including those operated on behalf of your organisation by partners and service providers) to ensure they are capable of operating in compliance with the DPA 2017.
	Ensure that automated decision-taking is lawful and explicit.

RECORD OF PROCESSING OPERATIONS

What you need to know on Records of Processing Operations (section 33 of the Data Protection Act)?

"Every controller or processor shall maintain a record of all processing operations under his or its responsibility."

1. What are the duties of controllers/processors with regard to records of processing?

Controllers and processors have a duty to document what personal data they hold, where it came from and how they share it with. The DPA requires you to maintain records of these processing activities. Each controller and processor is obliged to cooperate with the Data Protection Office and make those records, on request, available to it, for monitoring those processing operations.

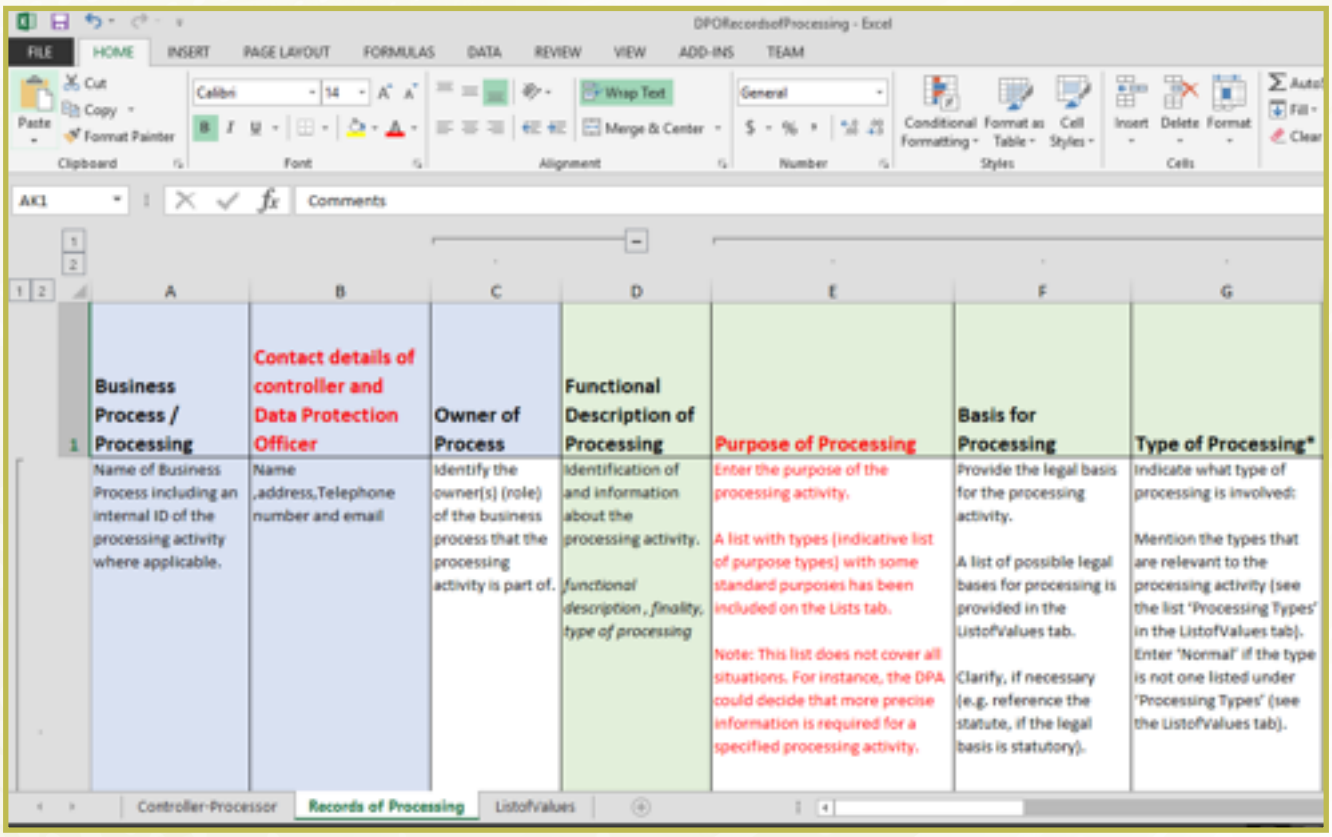
2. How to know what records to keep?

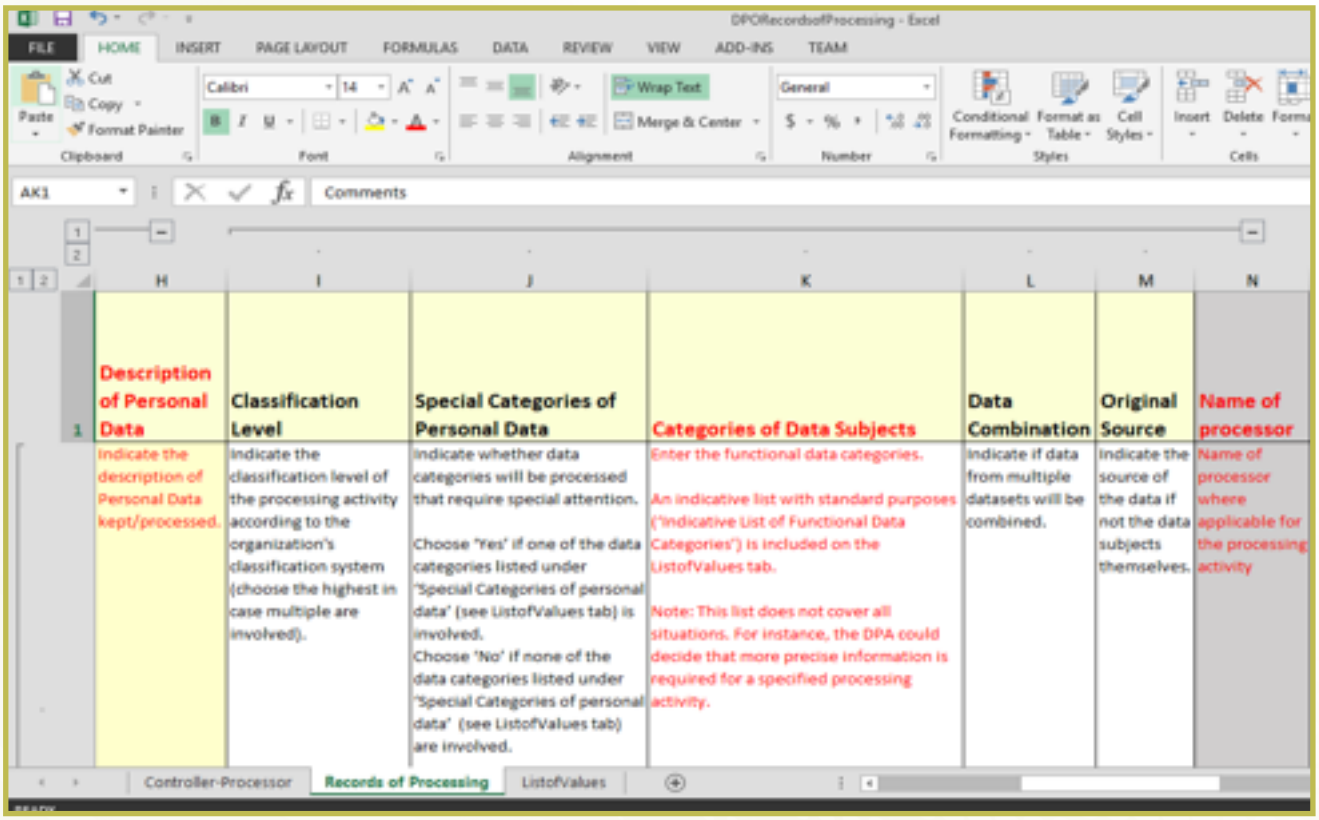
You may need to organise an information audit across the organisation or within particular business areas and ensure that all access to personal data are carried out with a particular business purpose.

3. How to keep the records?

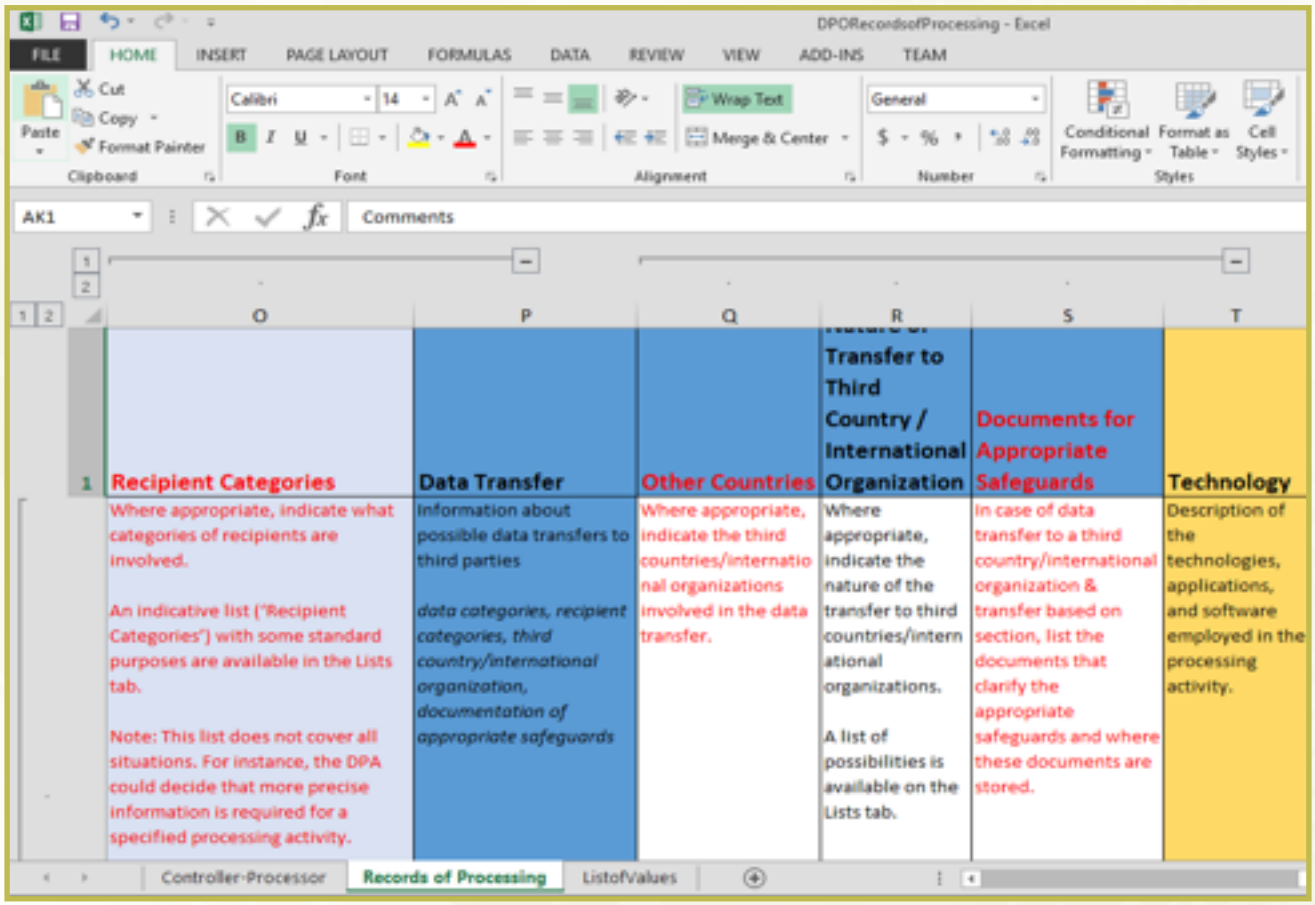
A template is provided for this purpose to ease the task of controllers and processors which is available on our website http://dataprotection.govmu.org/English/Pages/default.aspx under Documents and Forms section. You may use it or design your own one.

It consists of compulsory fields which have been highlighted in red and other useful fields to facilitate the task of the data protection officer. There is also a non-exhaustive list of possible values to assist in filling some of the fields. The following screen shots give an indication of the records of processing activities:

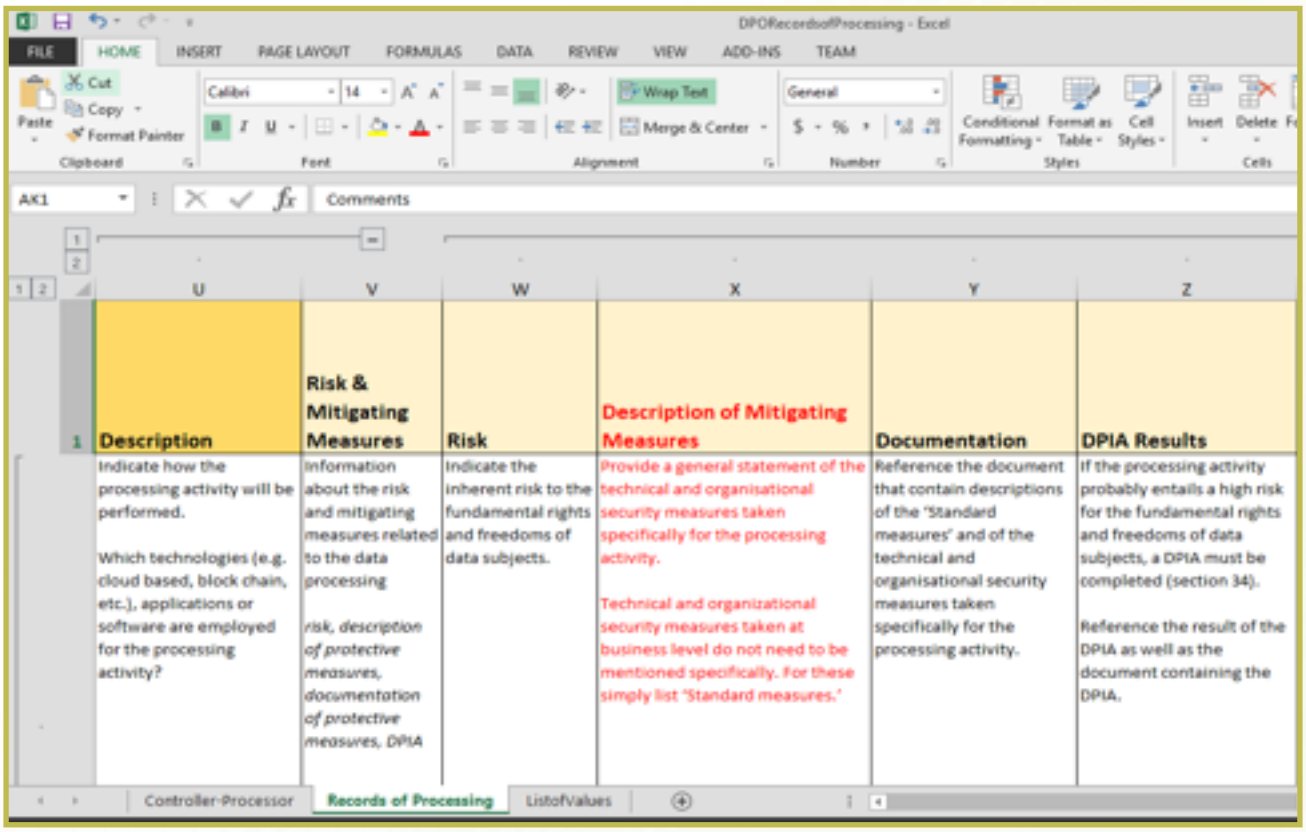




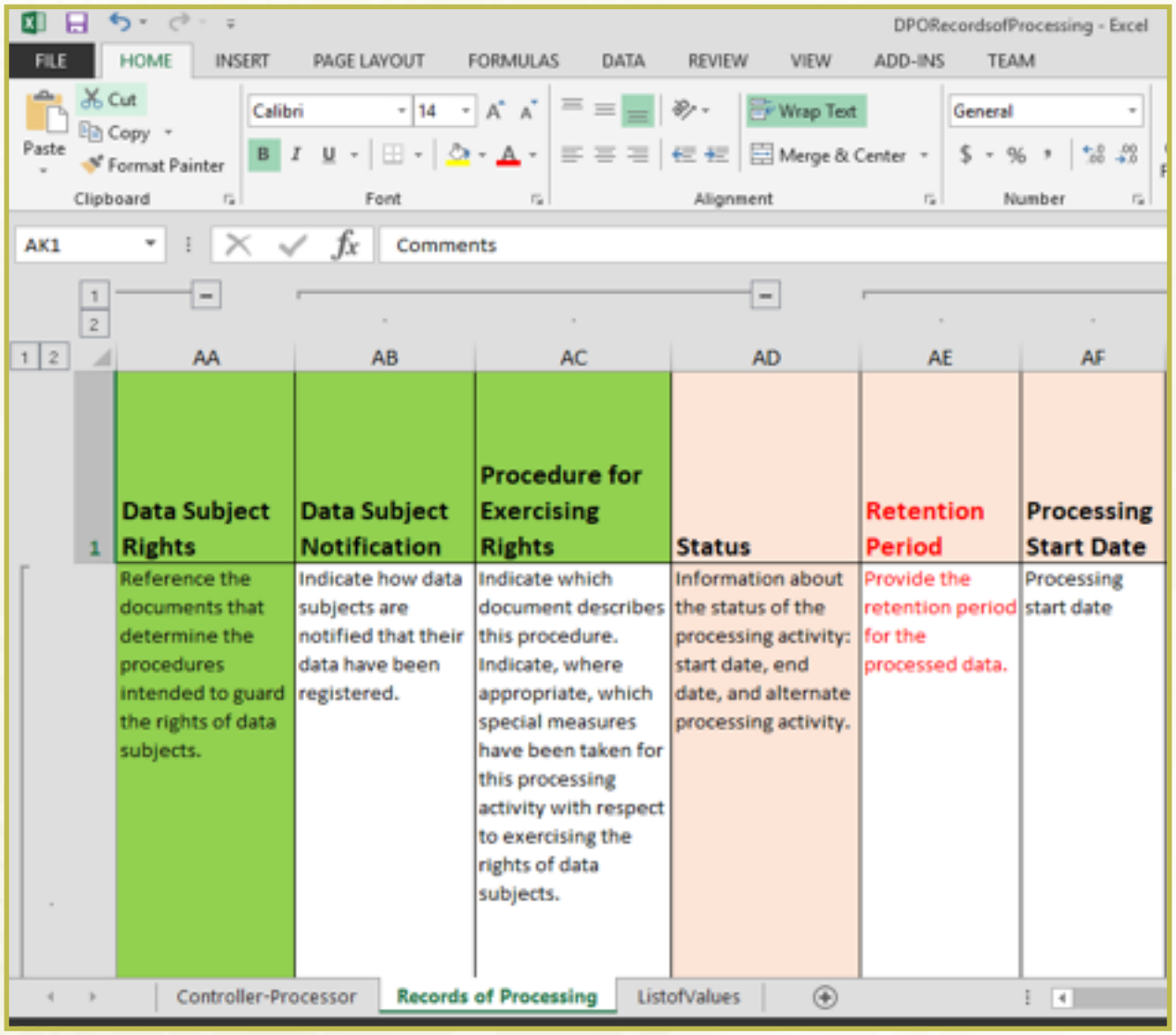
	H	I	J	K	L	M	N
1	**Description of Personal Data**	**Classification Level**	**Special Categories of Personal Data**	**Categories of Data Subjects**	**Data Combination**	**Original Source**	**Name of processor**
	Indicate the description of Personal Data kept/processed.	Indicate the classification level of the processing activity according to the organization's classification system (choose the highest in case multiple are involved).	Indicate whether data categories will be processed that require special attention. Choose 'Yes' if one of the data categories listed under 'Special Categories of personal data' (see ListofValues tab) is involved. Choose 'No' if none of the data categories listed under 'Special Categories of personal data' (see ListofValues tab) are involved.	Enter the functional data categories. An indicative list with standard purposes ('Indicative List of Functional Data Categories') is included on the ListofValues tab. Note: This list does not cover all situations. For instance, the DPA could decide that more precise information is required for a specified processing activity.	Indicate if data from multiple datasets will be combined.	Indicate the source of the data if not the data subjects themselves.	Name of processor where applicable for the processing activity



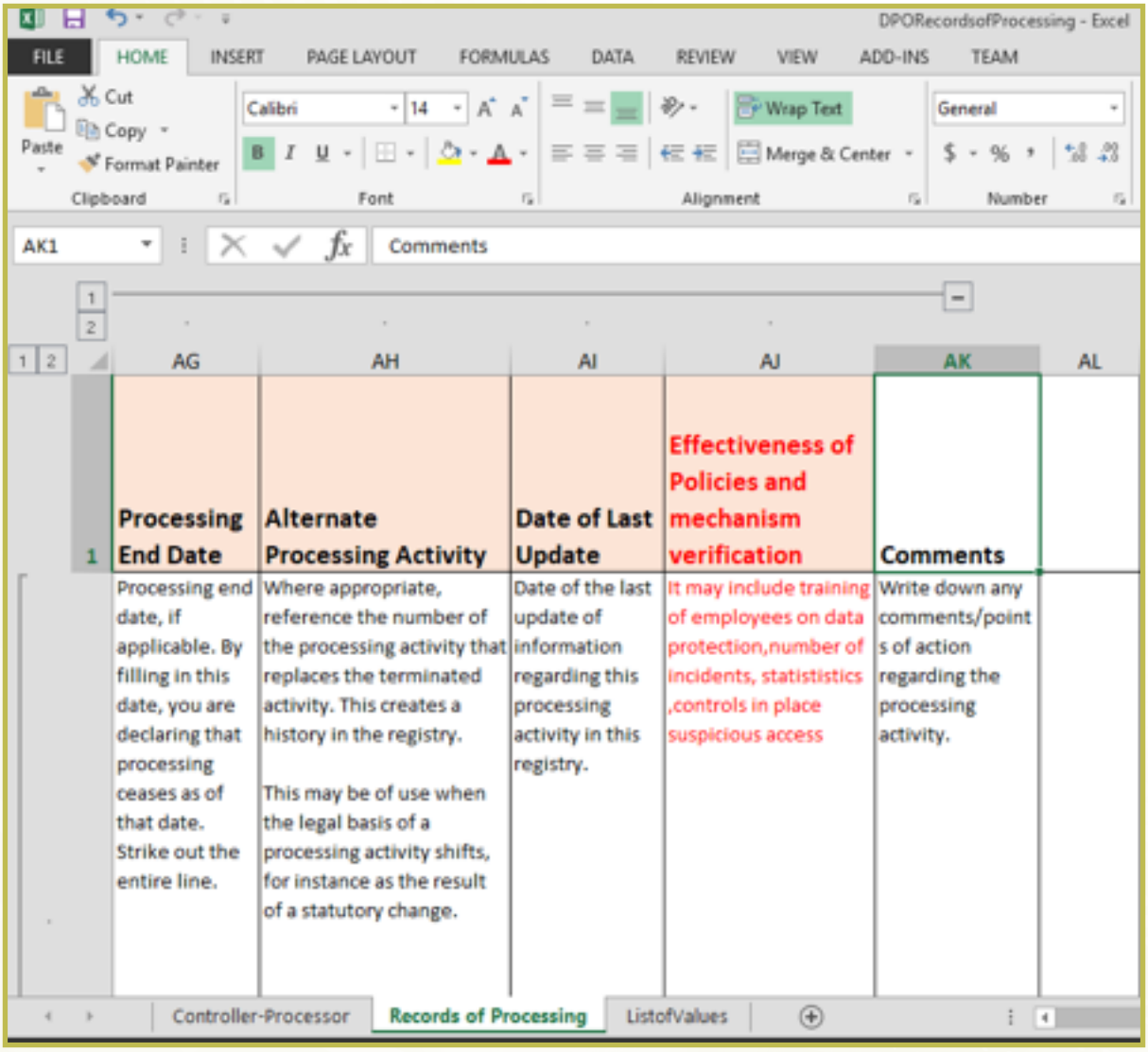
	O	P	Q	R	S	T
1	**Recipient Categories**	**Data Transfer**	**Other Countries**	**Transfer to Third Country / International Organization**	**Documents for Appropriate Safeguards**	**Technology**
	Where appropriate, indicate what categories of recipients are involved. An indicative list ("Recipient Categories") with some standard purposes are available in the Lists tab. Note: This list does not cover all situations. For instance, the DPA could decide that more precise information is required for a specified processing activity.	Information about possible data transfers to third parties *data categories, recipient categories, third country/international organization, documentation of appropriate safeguards*	Where appropriate, indicate the third countries/international organizations involved in the data transfer.	Where appropriate, indicate the nature of the transfer to third countries/international organizations. A list of possibilities is available on the Lists tab.	In case of data transfer to a third country/international organization & transfer based on section, list the documents that clarify the appropriate safeguards and where these documents are stored.	Description of the technologies, applications, and software employed in the processing activity.



	U	V	W	X	Y	Z
1	**Description**	**Risk & Mitigating Measures**	**Risk**	**Description of Mitigating Measures**	**Documentation**	**DPIA Results**
	Indicate how the processing activity will be performed. Which technologies (e.g. cloud based, block chain, etc.), applications or software are employed for the processing activity?	Information about the risk and mitigating measures related to the data processing *risk, description of protective measures, documentation of protective measures, DPIA*	Indicate the inherent risk to the fundamental rights and freedoms of data subjects.	Provide a general statement of the technical and organisational security measures taken specifically for the processing activity. Technical and organizational security measures taken at business level do not need to be mentioned specifically. For these simply list 'Standard measures.'	Reference the document that contain descriptions of the 'Standard measures' and of the technical and organisational security measures taken specifically for the processing activity.	If the processing activity probably entails a high risk for the fundamental rights and freedoms of data subjects, a DPIA must be completed (section 34). Reference the result of the DPIA as well as the document containing the DPIA.



	AA	AB	AC	AD	AE	AF
1	**Data Subject Rights**	**Data Subject Notification**	**Procedure for Exercising Rights**	**Status**	**Retention Period**	**Processing Start Date**
	Reference the documents that determine the procedures intended to guard the rights of data subjects.	Indicate how data subjects are notified that their data have been registered.	Indicate which document describes this procedure. Indicate, where appropriate, which special measures have been taken for this processing activity with respect to exercising the rights of data subjects.	Information about the status of the processing activity: start date, end date, and alternate processing activity.	Provide the retention period for the processed data.	Processing start date



Case scenario:

An organisation has the following business operations where personal data are processed: sales/ invoicing, marketing and finance.

Analysis:

After carrying an audit of the personal data processed, 3 rows of business process have to be filled for all the compulsory fields in the template provided. The other non-compulsory fields may be filled by the data protection officer.

4. Why keep these records?

Such records should be considered as one of the tools enabling the Data Protection Officer to perform his tasks of monitoring compliance, informing and advising the controller or the processor.

5. How to measure the effectiveness of policies and mechanisms?

Controllers and processors should have effective policies and procedures in place and communicate them to all employees. Training may need to be given to all employees to ensure that they understand the legal implications of unauthorised processing.

A fine-grained audit trail should be implemented in the organisation so that unauthorised access can be traced easily. Management reports may be viewed regularly to ensure compliance by employees.

Example: If you have inaccurate personal data and have shared this with another organisation, you will have to inform the other organisation about the inaccuracy so that it can correct its own records.

6. Is it an offence not to keep records of processing operation?

Yes, a controller/processor shall on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 5 years.

Record of processing operations

Main Points	To do list
It is an offence not to keep the records of processing operations and is liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 5 years	Make the records of processing operations available on request of the Data Protection office.
It may be required during an audit of the Data Protection Office.	Use the provided template or design your own. All compulsory fields have to be filled.
Keeping records of processing operations is compulsory.	Carry out an audit of the processing activities in the organisation.

LAWFUL PROCESSING

What you need to know on lawful processing (section 28 of the Data Protection Act)?

"no person shall process personal data unless -

a. the data subject consents to the processing for one or more specified purposes;

b. the processing is necessary - ……"

Section 28 of the Data Protection Act 2017 lays down the conditions that must be satisfied for processing of personal data to be lawful.

1. Do we need to consider the various types of data processing?

You must identify the lawful basis for your processing activity, document it and update your privacy notice to explain it. Under the Data Protection Act 2017, some individuals' rights will be modified depending on your lawful basis for processing their personal data.

Example: The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

2. Is it necessary to explain the lawful basis for processing personal data?

Yes you have to, especially when you have to answer an individual (a data subject) access request.

3. Do we need to review the types of processing operations?

You must be able to review the types of processing activities you carry out and to identify your lawful basis for doing so.

4. Why must we document our lawful bases?

You must document your lawful bases for processing in order to demonstrate compliance with the **"accountability principle"**. You are expected to put into place comprehensive but proportionate governance measures.

5. What needs to be considered for a new processing purpose?

A controller must consider assessing whether a new processing purpose is compatible with the purpose for which the data were initially collected. Where such processing is not based on consent, or on the provisions under sections 28(1)(b) and 44 of the Data Protection Act 2017, the following factors must be taken into account in order to determine compatibility:

a. any link between the original and proposed new purpose/s;
b. the context in which data have been collected (in particular the relationship between individuals and the controller);
c. the nature of the data (particularly whether they are special categories of personal data);
d. the possible consequences of the proposed processing; and
e. the existence of safeguards (including encryption or pseudonymisation).

6. Is there any specific fine applicable to lawful processing?

Yes, any person who contravenes section 28(1) shall be liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.

Lawful Processing:

Main Points	To do list
Section 28 sets out the conditions that must be satisfied for processing of personal data to be lawful.	You must ensure that the criteria for lawful processing can be monitored or met and verify whether these conditions are applicable.
There are new limitations on the use of consent and the processing of children's data.	Ensure that the quality of consent meets the new legal requirements (please refer to section 'consent' above).
There is a non-exhaustive list of factors to be considered when determining whether the processing of data for a new purpose is incompatible with the purposes for which the data were initially collected.	You must make sure that your internal governance processes will enable you to demonstrate how decisions to use data for further processing purposes have been reached and that relevant factors have been taken into account.

TRANSFER OF PERSONAL DATA OUTSIDE MAURITIUS

What you need to know on transfer of personal data outside Mauritius (section 36 of the Data Protection Act)?

"Controller or processor may transfer personal data to another country where –

(a) he or it has provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data;

(b) the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards;

(c) the transfer is necessary –

(i) for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

(iii) for reasons of public interest as provided by law;

(iv) for the establishment, exercise or defence of a legal claim; or

(v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(vi) for the purpose of compelling legitimate interests pursued by the controller or the processor which are not overridden by the interests, rights and freedoms of the data subjects involved and where –

(A) the transfer is not repetitive and concerns a limited number of data subjects; and

(B) the controller or processor has assessed all the circumstances surrounding the data transfer operation and has, based on such assessment, provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data; or

(d) the transfer is made from a register which, according to law, is intended to provide information to the public and which is open for consultation by the public or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down by law for consultation are fulfilled in the particular case."

1. When can personal data be transferred outside Mauritius?

Personal data may only be transferred outside of Mauritius in compliance with the conditions for transfer as set out in section 36 of the Data Protection Act.

2. What types of organisations are concerned?

All controllers and processors that engage in transfer outside Mauritius.

Example: Organisations using online IT services, cloud-based services, remote access services, global HR databases or organisations in the Business Process Outsourcing (BPO) sector, amongst others.

3. Does the country to which the data is transferred and the circumstances of the transfer ensure an adequate level of protection?

Having established that there is a transfer of personal data to another country, the controller or processor must then ask whether that country ensures an adequate level of protection to the personal data taking into account all the circumstances of the transfer.

4. Does this section apply if a business outsources one of its activities to a processor outside Mauritius?

Increasingly, controllers are using data processors in other countries to carry out processing on their behalf. A transfer to a data processor in that country will fall under this section.

Where a transfer is made to the processor in that country by the controller, the controller is still responsible for protecting individuals' rights under the Mauritian Data Protection Act.

5. Can the Commissioner prohibit a Transfer?

Yes. In order to protect the rights and fundamental freedoms of data subjects, the Commissioner may prohibit, suspend or subject the transfer to such conditions as he may determine.

6. Am I liable to any sanction/s if I do not comply with this section of the Data Protection Act?

Yes. Any person shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to imprisonment for a term not exceeding 5 years.

Transfer of Personal Data outside Mauritius

Main Points	To do list
Transfer of personal data to another country continue to be regulated under the new Act.	At the time of collection of personal data, inform the data subject of eventual transfer and the purpose/s for such transfer.
A controller or processor must provide proof of appropriate safeguards to the Commissioner before transferring personal data to another country.	Identify all circumstances in which personal data are transferred to recipients located outside Mauritius.
In the absence of appropriate safeguards, the data subject should provide his consent (explicit) after having been informed of the possible risks of the transfer.	Consider what security or other appropriate safeguards you have in place and whether these will continue to be necessary.
Section 36 (1) (c) provides other conditions where transfer can be made for example for the conclusion of contract, public interest requirements, amongst others.	Review questions included in standard procurement templates and contract clauses to ensure that information about your supplier's proposed transfer of personal data for which you are responsible is understood and conducted in a compliant way.
	Provide proof to the Data Protection Office regarding safeguards implemented for the transfer by filling in the Transfer of Personal Data Form, whenever required.

SECURITY OF PROCESSING

What you need to know on Security of Processing (section 31 of the Data Protection Act)?

"A controller or processor shall, at the time of the determination of the means for processing and at the time of the processing implement appropriate security and organisational measures for the prevention of unauthorised access to, the alteration of; the disclosure of; the accidental loss of; and the destruction of and the data in his control."

1. What does the Data Protection Act say about the security of processing?

The Data Protection Act says that:

Appropriate security and organisational measures shall be implemented for the prevention of unauthorised access to, the alteration of; the disclosure of; the accidental loss of; and the destruction of and the data in his control.

In practice, the Act requires personal data to be processed in a manner that ensures its security. Before deciding what level of security is right, there is a need to assess the risks to the personal data that the company is holding and choose security measures that are appropriate to the needs of the organisations.

Example: An organisation holds information about individuals' health which could cause damage or distress to those individuals if it fell into the hands of others. The organisation's information security measures should focus on any potential threat to the information or to the organisation's information systems.

2. Why should I worry about the security of personal data?

Information/ personal data security breaches may cause real harm and distress to the individuals they affect – lives may even be put at risk.

Example: The harm caused by the loss or abuse of personal data includes: identity fraud, fake credit card transactions, intimidation, etc.

3. What kind of security measures might be appropriate?

- Depending on the nature of processing, these measures may include:
- Pseudonymisation and encryption of the personal data;
- Maintaining ongoing confidentiality, integrity, availability, access, and resilience of processing systems and services.
- Restoring the availability of and access to personal data, in the event of a physical or technical incident;
- Testing and evaluating the effectiveness of technical and organisation measures.

4. What is pseudonymisation?

A new definition, which refers to the technique of processing personal data in such a way that it can no longer be attributed to a specific "data subject" without the use of additional information, which must be kept separately and be subject to technical and organisational measures to ensure non-attribution.

The use of pseudonymisation is encouraged, for instance on personal data served for historical scientific research or for statistical purposes

5. What is the position when a processor is involved?

Where a processor is involved, this often causes security problems. Particular care is needed because the controller will be held responsible under the Data Protection Act for what the processor does with the personal data.

Therefore, controllers should:

- ensure processors will treat their information securely - establish data processing contracts and ensure they contain necessary data protection related clauses;
- establish protocols to allow periodic security reviews of the security arrangements in place to provide assurances of compliance to contract/agreement; and
- if a processor is used to erase data and dispose of or recycle ICT equipment, make sure they do it adequately.

6. What should I do if there is a security breach?

Respond and manage the incident appropriately. This office recommends controllers and processors to have a policy on dealing with information security breaches. Refer to the part of on notification of a personal data breach for more information on how to handle a breach.

7. Am I liable to any sanction/s if I do not comply with this section of the Data Protection Act?

Yes. Any person shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to imprisonment for a term not exceeding 5 years.

Security to Processing

Main Points	To do list
Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate security (technical) or organisational measures.	A good starting point is to establish and implement a robust Information Security Policy which details the approach to: • information security(network and physical security, access controls, email and internet usage among others); • the technical and organisational measures that need to be implemented and • the roles and responsibilities staff have in relation to keeping information secure.
These measures include: pseudonymisation and encryption of the personal data; on-going reviews of security measures; redundancy and backup facilities; and regular security testing.	
When selecting a measure, the controller must have regard to these four criteria: the state of technological development available; costs, risks and nature of the data being processed.	Look to continually minimise the amount and type of data you collect, process and store, such as by undertaking regular information and internal process audits across appropriate areas of the business.
The Act contains special provisions when a processor is involved such as choosing a processor that provides sufficient guarantees about its security measures and written contracts to be signed.	Pseudonymise the personal data where appropriate to render the data record less identifying and therefore reduce concerns with data sharing and data retention.
Reasonable steps should be taken to ensure all staff is aware of, and complies with, the relevant security measures. For example: Training.	Create, review and improve your data security features and controls on an ongoing basis

DATA PROTECTION IMPACT ASSESSMENT

What you need to know on Data Protection Impact Assessment (section 28 of the Data Protection Act)?

"(1) Where processing operations are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature, scope, context and purposes, every controller or processor shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) The processing operations referred to in subsection (1) are - …….

(3) An assessment shall include - ……..

(4) Where appropriate, the controller or processor shall seek the views of data subjects on the intended processing……..."

A Privacy Impact Assessment (PIA) is seen as a valuable tool for businesses and governments as it enables them to make informed choices pertaining to privacy rights. It has always been good practice to adopt this tool as it assists organisations to determine effectively how personal data is being managed and processed. The Data Protection Act 2017 makes the PIA an express legal requirement, where the controller or processor needs to carry out an assessment of the impact of data processing.

Accordingly, a **Data Protection Impact Assessments (DPIA)**, also known as the Privacy Impact Assessment (PIA), is mandatory in certain circumstances, in other words, a DPIA is required in situations where data processing **is likely to result in high risk to the rights and freedoms of individuals**, for example (but is not limited to):

- where profiling operations are likely to significantly affect individuals;
- where there is processing on a large scale of special categories of data, for instance a hospital processing its patients' genetic and health data across all its branches (hospital information system); or
- where there is a systematic monitoring of a publicly accessible area on a large scale.

Example: Such processing operations may include a bank that screens its customers against a credit reference database, or a medical company offering genetic tests directly to consumers in order to assess and predict disease / health risks, or a new data processing technology is being introduced, or a company building behavioural or marketing profiles based on usage or navigation on its website.

1. What does a DPIA address?

- A DPIA can be useful for assessing multiple / single processing operations that are similar in terms of the risks presented, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing. This may also apply to scenarios where comparable technology is used to collect the same sort of data for the same purposes;

Example: A transport operator may cover video surveillance systems in all its stations / buses / trains with a single DPIA.

- A DPIA can be used to assess the data protection impact of a technology product, for example a piece of hardware or software. Thus, the controller developing or deploying the product remains obliged to perform its own DPIA. Nevertheless, other controllers using this particular product may also perform their own DPIA.

2. When is a DPIA not required?

- where the processing operation is likely to present lower levels of risk;

- if special categories of data, such as medical records, *are not processed systematically and on a large scale*, then, such processing operations may not automatically present high risks to the rights and freedoms of individuals;

Example: A medical doctor in a one-person practice may not be considered large scale or a company organising a corporate event and needs to know what kind of food the invitees are allergic to, may not carry out a DPIA.

- when the nature, scope, context and purposes of the processing are very similar to the processing for which a DPIA have already been carried out. In such cases, results of the DPIA for similar processing can be used;

- where the provisions under section 44 of the Data Protection Act 2017 are met.

  Nonetheless, in cases where it is not clear whether a DPIA is required, the Data Protection Office recommends that a DPIA is performed as it is a useful tool to help controllers or processors comply with data protection law.

3. Who will do the DPIA?

- Under section 34 of the Data Protection Act 2017, every controller or processor must perform an assessment of the impact of the envisaged processing activities on personal data being safeguarded.

- In cases where the processing operation involves controllers and processors, they will need to define their respective obligations precisely. Their DPIA must set out which party is responsible for the various measures designed to treat risks and to protect the rights and freedoms of individuals.

- If the processing is wholly or partly performed by a processor, then that processor must assist the controller in carrying out the DPIA. It may also be appropriate to seek the views of data subjects (individuals) in certain circumstances.

4. Who else needs to be involved?

Where a DPIA indicates that the processing may result in a high risk and the controllers or processors are unable to mitigate those risks by reasonable means, they will be required to consult the Data Protection Office to seek its opinion as to whether the processing operations comply with the Data Protection Act 2017.

5. At what moment a DPIA needs to be performed?

A DPIA must be carried out prior to processing, in other words, the DPIA must be started as early as practically possible in the design of the processing activities even if some of the processing operations are still unknown.

6. Why should we perform the DPIA as early as possible?

DPIA incorporates the principles relating to processing of personal data by taking into consideration privacy by design principles. It also fosters projects to be compliant with privacy and data protection at the outset to avoid potential breaches.

Likewise, privacy by design helps controllers and processors to comply with their obligations under the Data Protection Act.

Example: For instance, when building new IT systems for storing or accessing personal data, developing legislations / strategies that have privacy implications, or embarking on a data sharing initiative.

Privacy by design approach is an essential tool for minimising privacy risks and building trust as this can lead to increase awareness of privacy and data protection across a company.

7. When should we review a DPIA?

- where a significant change to the processing operations have occurred, for example a new technology has been implemented or personal data is being used for different purpose/s. In these instances, the processing in effect becomes a new data processing operation and may require a DPIA;

- when the context or components of processing operations evolve, for instance the functionalities, purposes, risk sources, new vulnerabilities / threats may arise or there is a change of the risks presented by the processing operations.

- in cases where the organisational context for the processing activity has changed, such as personal data is intended to be transferred outside Mauritius and such data is likely to present high risks, or effects of some automated decisions have become more significant, or new categories of individuals become vulnerable to discrimination.

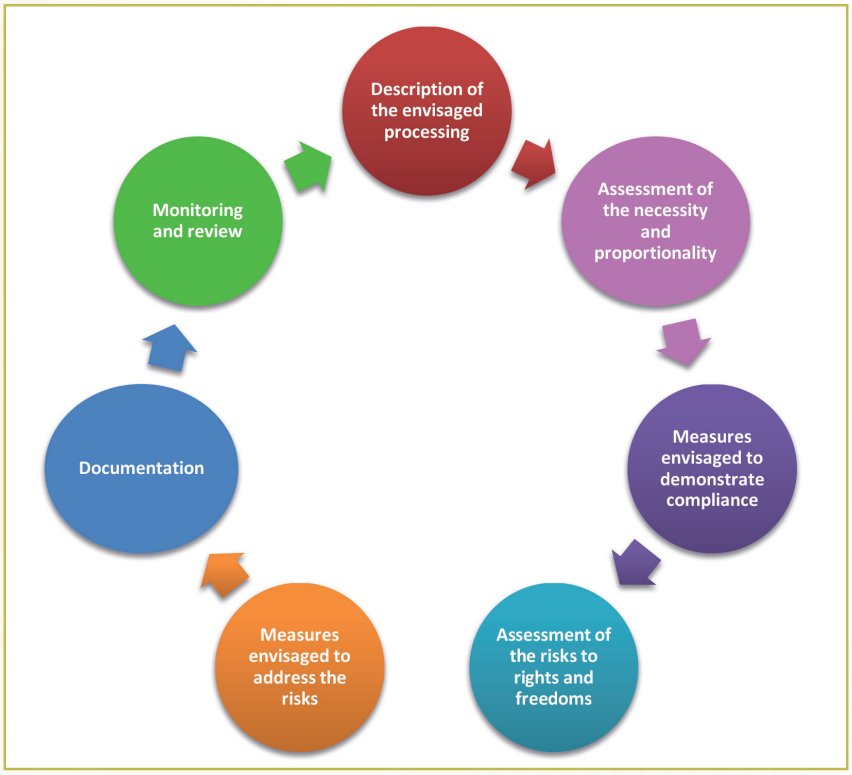
In general, it is a good practice to continuously perform a DPIA on existing processing activities. Nevertheless, depending on the nature of the processing as well as the rate of change in the processing operations or any other circumstances and the risks for the rights and freedoms are still mitigated, a DPIA may be re-assessed after 3 years, for instance the use of intelligent video analysis systems to automatically recognise license plates.

In some cases the DPIA will be an on-going process, for example where a processing operation is dynamic and subject to ongoing change. A DPIA must be carried out on a continual process and not a one-time exercise.

8. How to perform a DPIA?

- The Data Protection Act 2017 sets out the minimum features of a DPIA:
  a. a description of the envisaged processing operations and the purposes of the processing;
  b. an assessment of the necessity and proportionality of the processing;
  c. an assessment of the risks to the rights and freedoms of data subjects;
  d. the measures envisaged must address:
     i. the risks and the safeguards, security measures, mechanisms to ensure protection of personal data;
     ii. demonstrate compliance with the Data Protection Act 2017.

- The following figure demonstrates the iterative process for carrying out a DPIA:



- In risk management terms, a DPIA aims at "managing risks" to the rights and freedoms of natural persons, using the following three processes, by:

  a. establishing the context: taking into account the nature, scope, context and purposes of the processing and the sources of the risk;
  b. assessing the risks: assess the particular likelihood and severity of the high risk;
  c. treating the risk: mitigating that risk and ensuring the protection of personal data, and demonstrating compliance with the Data Protection Act 2017.

9. What is the best methodology to carry out the DPIA?

- The Data Protection Act 2017 provides controllers or processors with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices. However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers or processors to take measures to address them.

- There are a number of different methodologies that can be used to assist in the implementation of the basic requirements set out in the Data Protection Act 2017. However, any criteria that have been used must meet the standards required by the Data Protection Act 2017.

- The Data Protection Office has designed a "Data Protection Impact Assessment Questionnaire" that can help controllers or processors to assess their compliance status. Furthermore, this office will also publish a list of processing operations where a DPIA will be considered mandatory.

- Controllers or processors are encouraged to familiarise themselves with the Privacy Compliance Assessment Web Application (PCA Web App) which is available on this office's website http://dataprotection.govmu.org/English/Publications/Pages/Privacy-Compliance-Assessment.aspx. This PCA Web App comprises simple questions and multiple choice answers with the purpose to obtain a complete picture of the structure of personal information flows within an organisation so that appropriate compliance procedures can be put in place to ensure that the organisation deals with personal data in accordance with data protection legislations and best practices.

Data Protection Impact Assessment (DPIA):

Main Points	To do list
A DPIA is required in situations where data processing is likely to result in high risks to individuals.	You must start to assess the situations where it will be necessary to conduct a DPIA.
Businesses have a general obligation to implement appropriate technical and organisational measures to show that they have considered and integrated data protection into their processing activities.	You must adopt internal policies and implement measures which help your organisations comply with the principles relating to processing of personal data.
DPIA can help you identify the most effective way to comply with your data protection obligations and meet individuals' expectations of privacy.	It is recommended that you undertake a DPIA in cases where it is unclear whether doing so is required. An effective DPIA will allow you to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.
If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks.	You will be required to consult the Data Protection Office to seek its opinion as to whether the processing operation complies with the Data Protection Act 2017.
The Data Protection Office will publish a list of processing operations where DPIA will be mandatory and has designed a "Data Protection Impact Assessment Questionnaire" that can help controllers or processors to assess their compliance status.	You familiarise yourself with the Privacy Compliance Assessment Web Application (PCA Web App) which is available on this office's website.

PRIOR AUTHORISATION AND CONSULTATION

What you need to know on prior authorisation and consultation (section 35 of the Data Protection Act)?

"Every controller or processor shall obtain authorisation from the Office prior to processing personal data in order to ensure compliance of the intended processing with this Act and in particular to mitigate the risks involved for the data subjects where a controller or processor cannot provide for the appropriate safeguards referred to in section 36 in relation to the transfer of personal data to another country."

1. When shall authorisation be sought from the Data Protection Office?

When a processing operation is likely to result in a high risk to the rights and freedoms of an individual or where a controller or processor cannot provide for the appropriate safeguards referred to in section 36 in relation to the transfer of personal data to another country.

Example: The processing of health data on a large scale is considered as likely to result in a high risk.

2. Should I provide the Data Protection Impact Assessment to the Data Protection Office?

Yes. This should be provided in order to allow the Office to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards where the DPIA indicates high risk to the rights and freedoms of data subject.

Prior authorisation and consultation

Main Points	To do list
Controller or processor must obtain authorisation from the Office prior to processing personal data in order to ensure compliance of the intended processing with the Act and in particular to mitigate the risks involved for the data subjects where it cannot provide for the appropriate safeguards referred to in section transfer of personal data outside Mauritius.	Identify your responsibilities as controller and processor who are involved in the processing.
	Determine the purposes and means of the intended processing.
	Perform a data protection impact assessment provided for in section 34.
The Office may prohibit the intended processing if it is of the view that the intended processing does not comply with the Act, in particular where risks are insufficiently identified or mitigated.	Communicate the above information to the Data Protection Office and be ready to provide other information.

REGISTRATION OF CONTROLLERS

What you need to know on Registration of Controllers (sections 14-20 of the Data Protection Act)?

"... no person shall act as controller or processor unless he or it is registered with the Commissioner..."

1. Why do I have to register?

Section 14 of the Data Protection Act clearly makes it a legal requirement for controllers to register with the Data Protection Office.

2. Am I liable to any sanction/s if I do not comply with the registration requirement of the Data Protection Act?

Yes. Any person shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to imprisonment for a term not exceeding 5 years.

3. Who should register?

By definition a "controller" means a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing.

Example: A school, medical practitioner, société, barrister, ministry, public bodies, private companies such as insurance company/bank, amongst others

4. Do I have to register if I am a dormant company?

Yes in most cases. For instance, you may have personal data of shareholders and directors (non-salaried). In the case that you are a one-man business and dormant, you need to seek advice specific to your circumstances regarding registration with the Data Protection Office.

5. How do I register?

The 'Controller Application Form for registration' available on the office website at http://dataprotection.govmu.org must be completed and sent to the Data Protection Commissioner. The form includes the following:

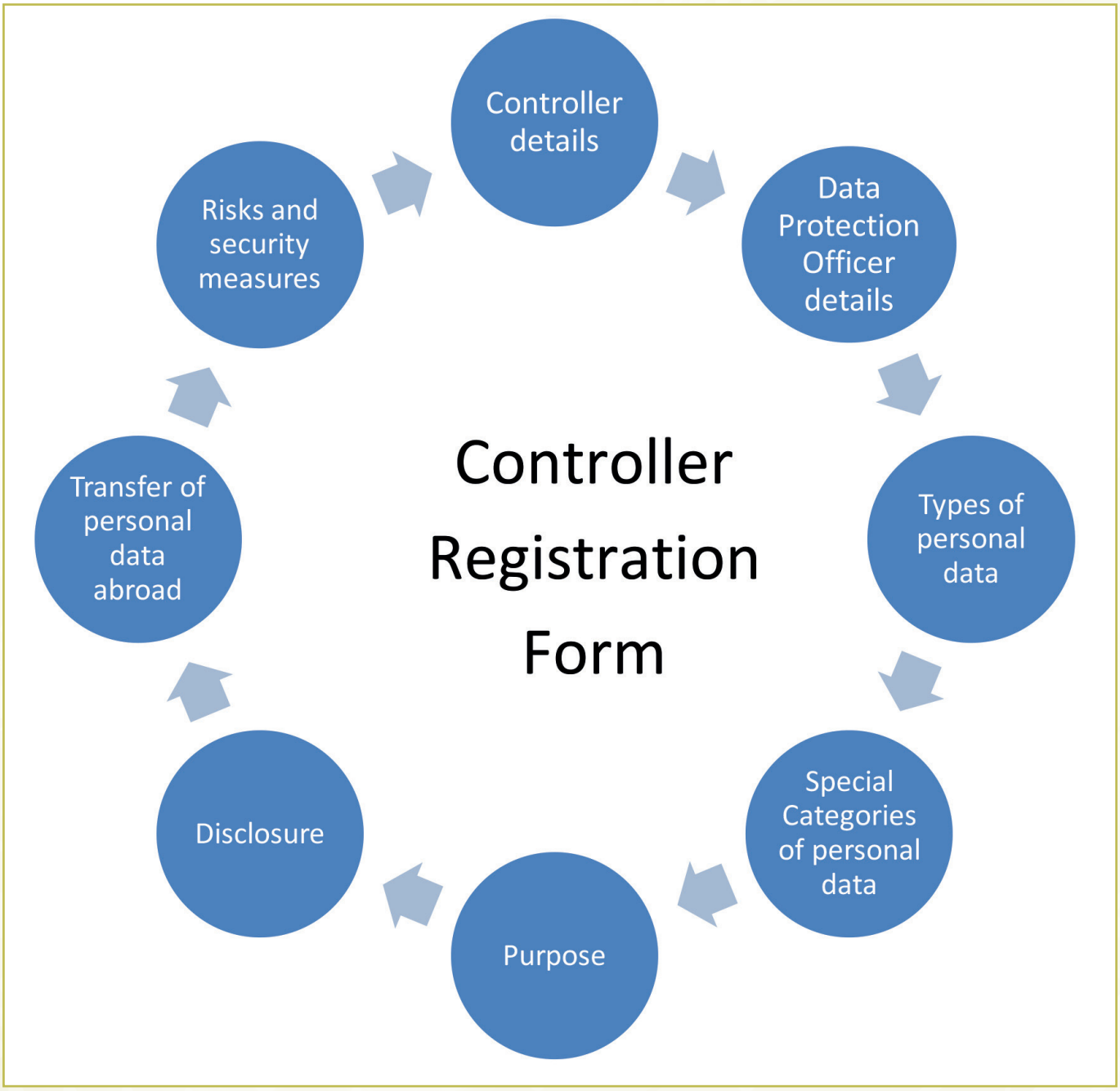


Figure 1: Particulars of Controller Application Form

6. If I have 100 employees or 10000 customers, do I have to list each one of them in the form?

No. You do not have to give actual names of people in the form. Rather, you have to list the DESCRIPTION/TYPES of personal data. For example, name, national identity card number, qualification, fingerprint data, car number, bank account number, amongst others, are types of data.

Case Scenario:

Example: A school has 50 teachers and 800 students. When a teacher is appointed at the school, he needs to submit his/her name, copy of National Identity Card Number, qualification details, bank account number, copy of birth certificate and curriculum vitae which is kept by the Human Resource Department. Similarly, when a student is admitted to the school, the student provides his/her name, the name of his/her parents and a copy of his/her birth certificate which are recorded in the student's database at the school.

Analysis:

When the school registers as Controller with the Data Protection Office, the school will provide ONLY the types of information kept in the section 'Description of personal data processed' as follows:

Staff - Name, National Identity card number, qualification, bank account number, birth certificate, curriculum vitae.

Students – name of student, name of parents, birth certificate.

7. Am I liable to any sanction/s if I provide any false or misleading information when providing the particulars in the Controller Application Form?

Yes. A controller shall on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 5 years.

8. Do I need to pay when I register?

Yes. The fees payable are available on the office website at http://dataprotection.govmu.org.

9. How do I receive a registration certificate?

After being duly registered as controller with the Data Protection Office, you will be issued a registration certificate in such form and manner as the Commissioner may determine.

10. What is the validity period of a registration certificate?

The registration certificate is valid for 3 years.

11. Is the registration certificate renewable after 3 years?

Yes. You may apply for renewal of the registration certificate not later than 3 months before the date of its expiry. The Commissioner shall, on such terms and conditions as prescribed and on payment of such fee as prescribed, issue the new registration certificate to you.

12. Can the Commissioner cancel or vary the terms and conditions of a registration certificate?

Yes, subject to certain conditions. However, prior to cancelling or varying the terms and conditions of the certificate, the Commissisoner will require by notice in writing the holder of a certificate to show cause within 14 days of the notice why the registration certificate should not be cancelled or its terms and conditions should not be varied.

13. What happens if there are any change in particulars after I have registered, such as change of name?

The controller must notify the Commissioner in writing of the nature and date of the change within 14 days of the date of the change.

14. What happens if I do not notify any change in particulars to the Data Protection Office?

The controller shall, on conviction, be liable to a fine not exceeding 50,000 rupees.

15. Does the Data Protection Office keep a list of registered controllers?

Yes. The Data Protection Commissioner keeps and maintains a Data Protection Register of controllers. The register shall at all reasonable times be available for inspection by any person free of charge. Any person may also on payment of a prescribed fee obtain a certified copy of or an extract from any entry in the register.

Registration of controllers

Main Points	To do list
Registration of controllers is compulsory under the Data Protection Act.	Review and make a list of all types of personal data being processed.
Controllers must submit 'Controller Application Form for registration' to the Data Protection Office.	Ensure you have adequate security measures to protect personal data. Additional safeguards must be implemented for special categories of personal data.
After being registered as controller, a registration certificate is issued.	Ensure all disclosures of personal data are carried out in accordance with the Data Protection Act.
The registration certificate is valid for 3 years and is renewed on payment of a prescribed fee not later than 3 months before the date of expiry.	Designate an officer responsible for data protection compliance issues.
The Commissioner may under certain circumstances cancel or vary the terms and conditions of a registration certificate.	Ensure data is processed according to the purpose specified.
Controllers must notify the Commissioner in writing of any change in particulars within 14 days of the date of the change.	Check that transfers for personal data abroad are in compliance with the Data Protection Act.
The Commissioner keeps and maintains a register of controllers.	Verify that your registration and renewal obligations as controller are up to date.

REGISTRATION OF PROCESSORS

What you need to know on Registration of Processors (sections 14-20 of the Data Protection Act)?

"... no person shall act as controller or processor unless he or it is registered with the Commissioner."

"Processor" *means a person who, or public body which, processes personal data on behalf of a controller.*

Example: Company 'XYZ' is involved in e-commerce business. All servers of Company 'XYZ' are hosted locally by Company 'ABC' in its data centre and the latter manages the servers on behalf of Company 'XYZ'. Therefore, Company 'ABC' is the processor and Company 'XYZ' is the controller.

Part III of the Data Protection Act 2017 lays down the conditions for registration of controllers and processors. Thus, a processor shall, pursuant to section 14 of the new Data Protection Act, register with the Data Protection Office.

Please refer to section 'Controller Registration' (above) for additional information regarding 'Registration of Processors' as same principles apply under sections 14 to 20 of the Data Protection Act 2017. In this part we will cover specific items pertaining to processors only.

1. I'm already registered as a controller, should I register as a processor?

- In case you are processing personal data on behalf of a controller, you must register as a processor with the Data Protection Office. As per example above, Company 'ABC' must also register as processor with this office.

2. What are my obligations as a processor?

- You must comply with Part IV of the Data Protection Act 2017, thereby ensuring (amongst others):

  a. implementation of appropriate security and organisational measures;
  b. provision of sufficient guarantees in respect of security and organisational measures;
  c. a written contract which needs to provide that:
     i. the processor shall act only on instructions received from the controller; and
     ii. the processor shall be bound by obligations devolving on the controller under section 31(1) of the Data Protection Act 2017
  d. that any person employed by the controller or processor are aware of and comply with relevant security measures.

3. What happens if a processor processes personal data other than instructed by a controller?

The processor will be considered to be a controller in respect of that processing.

ROLES OF DATA PROTECTION OFFICER

What you need to know on data protection officer? (Section 22 2(e) of the Data Protection Act)?

"(1) Every controller shall adopt policies and implement appropriate technical and organisational measures so as to ensure and be able to demonstrate that the processing of personal data is performed in accordance with this Act.

(2) The measures referred to in subsection (1) shall include –

(a) implementing appropriate data security and organisational measures in accordance with section 31;
(b) keeping a record of all processing operations in accordance with section 33;
(c) performing a data protection impact assessment in accordance with section 34;
(d) complying with the requirements for prior authorisation from, or consultation with the Commissioner pursuant to section 35; and
(e) designating an officer responsible for data protection compliance issues"

1. Is it mandatory to appoint a data protection officer in the organisation?

Yes. According to section 22 (2) (e) of the Data Protection Act, controllers and processors shall designate an officer responsible for data protection compliance issues.

2. What are the roles of the data protection officer?

The data protection officer should work independently, report to the highest management level and have adequate resources to enable the controller or the processor to meet its obligations under the Data Protection Act.

The following illustrates the minimum tasks that a Data Protection Officer should carry out. However the controller/processor can add on more tasks to meet their business requirements:

- Inform and advise the controller/processor and its employees about their obligations to comply with the DPA and other data protection laws.
- Monitor compliance with the DPA and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits.
- Be the first point of contact for the Data Protection Office and for individuals whose data are processed (employees, customers, amongst others).

3. Can we allocate the role of data protection officer to an existing employee?

Yes. As long as the professional duties of the employee are compatible with the duties of the data protection officer and do not lead to a conflict of interests.

Controller/processor can also contract out the duties of the data protection officer externally subject to a rigorous contract establishing appropriate safeguards regarding protection of personal data processed by the controller/processor.

4. Does the data protection officer need specific qualifications?

The Data Protection Act does not specify the qualifications a data protection officer is expected to have, however, this office recommends that a data protection officer should have professional experience and knowledge of data protection laws. This should be proportionate to the type/s of processing your organisation carries out, taking into consideration the level of protection the personal data requires.

Roles of Data Protection Officer

Main Points	To do list
Appointing a data protection officer is mandatory.	Determine whether to appoint a data protection officer and define his role.
A single data protection officer may be appointed for a group of companies depending on their structure and size.	Establish who the data protection officer should report to, most preferably the management level i.e. the board.
A data protection officer operates independently and is not to be dismissed or penalised for performing their tasks.	Adequate resources are to be provided to enable data protection officer(s) to meet the company's obligations under the Act.

NOTIFICATION OF PERSONAL DATA BREACH AND COMMUNICATION TO DATA SUBJECT

What you need to know on notification of a personal data breach and communication to data subject (sections 25 and 26 of the Data Protection Act)?

"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner..."

"Subject to subsection (3), where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the controller shall, after the notification referred to in section 25, communicate the personal data breach to the data subject without undue delay..."

1. What is a personal data breach?

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.

Example: An intruder steals a device containing a controller's customer database and misuses it to impersonate the customers.

2. When does a controller/processor becomes "aware" of a personal data breach?

Sometimes, it might be clear right from start whilst at other times, a quick preliminary investigation will help to determine whether a breach has occurred. It can be associated to a point where the controller has a reasonable degree of certainty that a breach has occurred. The focus is to take prompt action to investigate whether a breach has occurred or not.

Example: A controller suspects that his network has been accessed by an intruder. He quickly verifies and finds that his data has been compromised. Clearly, the controller is now 'aware' of a personal data breach.

3. What is the obligation of processors?

To notify the controller without any undue delay as soon as the processor becomes aware of the personal data breach.

4. What is the obligation of controllers?

Action	Timing
1. To notify the personal data breach to the Data Protection Commissioner.	Without undue delay and, where feasible, not later than 72 hours after having become aware of it.
2. To communicate the personal data breach to the data subject where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject. (Note: Please also check the circumstances where communication to data subjects is not required as described at point 8 below.)	Without undue delay after notifying the Data Protection Commissioner.

5. What happens if I cannot meet the timing delay of 72 hours to report to the Data Protection Commissioner?

Reasons for the delay will have to be provided to the Data Protection Commissioner.

6. How do I report a personal data breach to the Data Protection Commissioner?

The 'Personal Data Breach Notification Form' available on the office website at http://dataprotection.govmu.org must be completed and sent to the Data Protection Commissioner.

The form includes prescribed requirements such as nature of the personal data breach, including where possible, the categories and approximate number of data subjects and the categories and approximate number of personal data records concerned, contact details of a contact point and the measures to address the breach and to mitigate the adverse effects of the breach.

It is to be noted that after a controller submits a notification to the Data Protection Office, if the controller finds some further evidence that he deems necessary to communicate to the Office or the controller finds that there was no breach itself, the controller should update the Data Protection Office in light of new findings.

7. How can a communication to a data subject be made?

Describe in clear language the nature of the personal data breach and the facts relating to the personal data breach, its effects and the remedial action taken.

8. Are there circumstances where communication to data subjects is NOT required?

Yes. Communication to data subjects is not required when:

- Appropriate technical and organisational protection measures were already in place before the breach occurred such as encryption techniques which rendered the data unintelligible to any person not authorised to access it;
- The controller has taken subsequent measures to ensure that the breach is unlikely to result in a high risk to the rights and freedoms of the data subjects. The controller at this stage can also refer to the Data Protection Impact Assessment carried out to verify the potential harm;
- It would involve disproportionate effort and the controller has made a public communication or similar measure whereby a data subject is informed in an equally effective manner.

9. Am I liable to any sanction/s if I do not comply with the notification of a personal data breach requirement of the Data Protection Act?

Yes. Any person shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to imprisonment for a term not exceeding 5 years.

In addition to any penalty referred to above, the Court may –

- order the forfeiture of any equipment or any article used or connected in any way with the commission of an offence;
- order or prohibit the doing of any act to stop a continuing contravention.

Notification of personal data breach and communication to data subject

Main Points	To do list
A processor must report a personal data breach to the controller.	Make sure you have appropriate technical and organisational protection measures to protect data and also adequate techniques such as encryption to minimise the adverse effect of a breach.
Controllers must report the personal data breach to the Data Protection Commissioner and in certain circumstances to data subjects.	Determine whether to set up a breach response team for addressing incident identification systems and incident response plans.
There are is a time limit for reporting a personal data breach to the Data Protection Commissioner.	To regularly review and update all procedures for addressing breaches.
Reasons for any delay in reporting the breach must be provided to the Data Protection Commissioner.	Be careful not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action.
There are some specific cases where controllers do not have to communicate the personal data breach to data subjects.	Determine whether any other external third party/ies need to be notified to limit the potential impact.
Controllers must submit the 'Personal Data Breach Notification Form' to report to the Data Protection Commissioner.	Determine whether a review of employee training practices is required.
	Document all information regarding the breach to avoid any re-occurrence.

CERTIFICATION

What you need to know on Certifications (section 48 of the Data Protection Act)?

1. What is the purpose of a certification mechanism?

The concept of certifying data processing operations is a significant development in creating a reliable and auditable framework for data processing operations.

A certification mechanism is a way of demonstrating that you comply, in particular, showing that you are implementing technical and organisational measures.

A certification mechanism may also be established to demonstrate the existence of appropriate safeguards related to the adequacy of data transfers.

They are intended to allow individuals to quickly assess the level of data protection of a particular product or service.

2. Am I liable to any sanction/s if I do not obtain the certification under the Data Protection Act?

No. Certifications are voluntary. Recommendations will be issued by the Data Protection Office for ensuring compliance unless other sections of the Data Protection Act have been breached.

3. Does the absence of certification or failure in receiving certification have any negative effect on the controllers or processors?

Having no certification does not mean that an organisation is less likely to be compliant. However the goodwill of the company may be affected.

In addition, being unsuccessful in receiving a certification from the DPO or generally withdrawing from the certification application process is not sanctioned by the DPO, nor in itself carries negative inferences with respect to compliance.

4. Who is responsible for certification mechanisms?

The Data Protection Office encourages the establishment of certification mechanisms to enhance transparency and compliance with the Data Protection Act 2017.

Certifications will be issued by the Data Protection Office.

5. How do I apply for certification?

The application form is available on the office website. While filling in the application form, controllers or processors must provide all relevant information about processing activities they seek to certify, type/s of personal data, details about processing purpose, organizational and security measures in place to enable the Data Protection Office to conduct the certification procedure. Subsequently, the Data Protection Office will arrange for an audit with the controllers or processors.

6. Do I need to pay when I apply for certification?

No. Certifications are free.

7. What does the certification process consist of?

The data protection officers will conduct an audit on the arranged date at the controllers' or processors' premises to verify whether the controllers' or processors' processing activities comply with the Data Protection Act. Following the audit, the data protection officers will write a report about their findings and will decide if certifications can be granted. If yes, certification with seal will be remitted to the controllers or processors.

Otherwise, corrective actions will be recommended to the controllers or processors to be implemented in a number of days.

8. What is the validity period of a certification?

A certification is valid for 3 years.

9. Is the certification renewable after 3 years?

Yes. You may apply for renewal of the certification before the date of its expiry.

10. Can the certification be cancelled?

Certifications are subject to withdrawal where the conditions for issuing the certificates are no longer met.

11. What are the benefits of certifications?

Benefits for individuals
Certifications carry tangible benefits for individuals.

- **Create trust**

Certifications have the potential of increasing individuals' trust and confidence in a certified organisation's handling of their personal data. This in turn may result in individuals' wanting to engage more with a certified organisation and participating in the digital economy more freely.

- **Greater transparency**

Certification ensures better transparency of processing practices of the organisation, making it easier for individuals to understand and assess relevant data practices and their merits.

- **Effective privacy protection**

Individuals may regard certification as a demonstration of commitment to and compliance with effective and rigorous data protection and complaint resolution practices. Adherence to certification mechanisms by organisations ultimately may deliver better compliance and outcome for individuals, with their data being more effectively protected.

Benefits for Certified Organisations
If implemented effectively, certifications may convey a number of key benefits to organisations.

- **Demonstrate accountability and compliance**

Certification is an element of demonstrating compliance and accountability with the Data Protection Act 2017. This is an internal benefit vis-à-vis management, the board and shareholders. It also benefits an organisation externally in its relationships with the Data Protection Office, individuals, clients and business partners. It builds confidence and trust in the organisation with these external stakeholders, as well as with the wider public.

- **Enabling cross-border data transfers**

Certified organisations are recognised as providing adequate privacy protection thus giving legal certainty for cross-border data transfers. This particularly eases business for the ICT-BPO industry, in particular in terms of free flow of data from EU or other parts of the world to Mauritius.

Certifications

Main Points	To do list
The Data Protection Office encourages the establishment of data protection certification mechanisms, seals and marks.	Controllers or processors wishing to be certified must apply for certification with the Data Protection Office.
Certifications are voluntary but enable controllers and processors to demonstrate compliance with the Data Protection Act.	
Certificates will be issued by the Data Protection Office.	
Certifications will be valid for three years and subject to renewal.	
Certifications will be withdrawn if the requirements of the certification are no longer met.	

COMPLAINTS (PROCESS OF COMPLAINTS)

What you need to know on Complaints (section 6 of the Data Protection Act)?

"Where a complaint is made to the Commissioner that this Act or any regulations made under it, has or have been, is or are being, or is or are about to be, contravened, the Commissioner shall –

(a) investigate into the complaint or cause it to be investigated by an authorised officer, unless he is of the opinion that the complaint is frivolous or vexatious; and

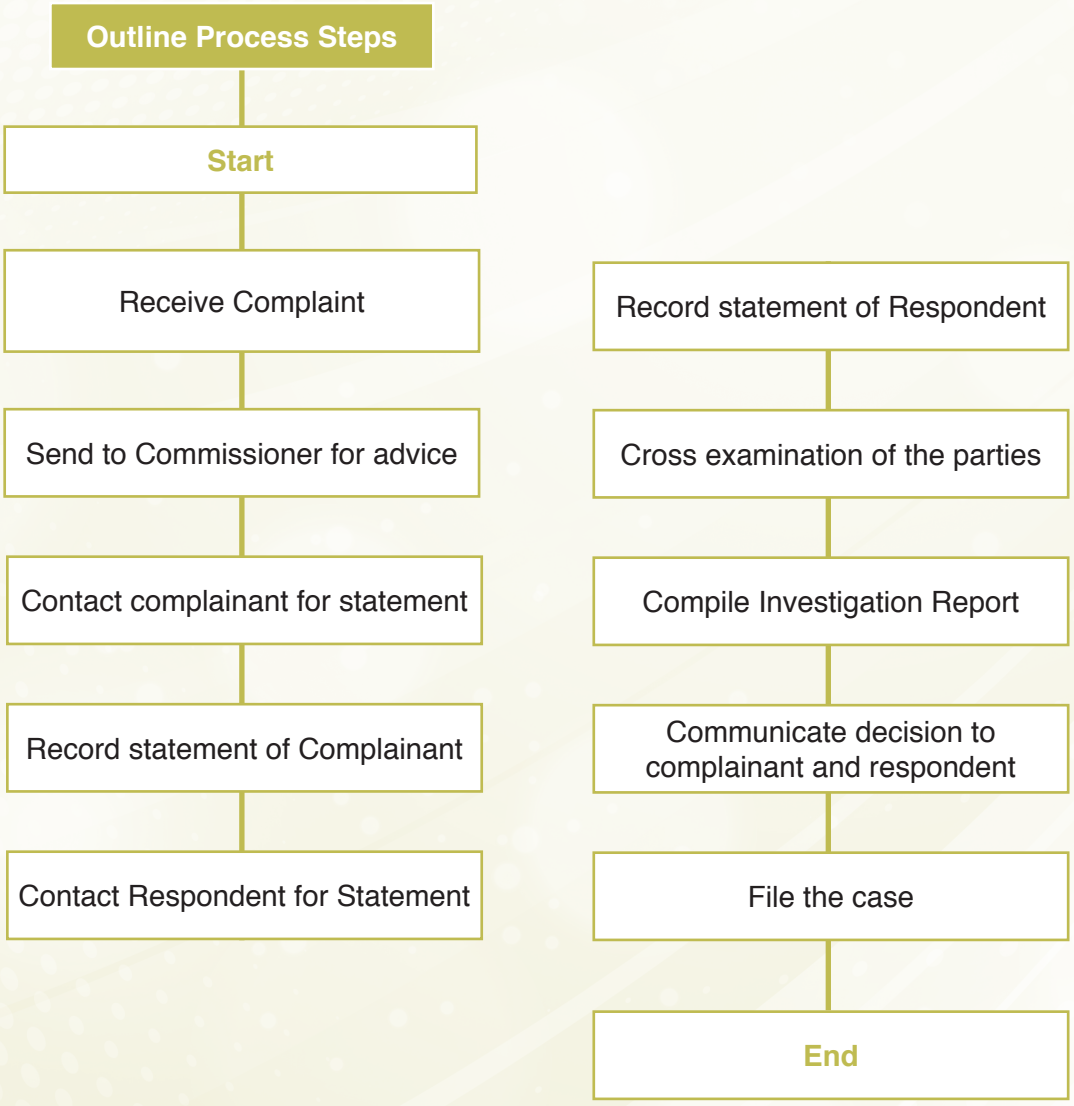
(b) where he is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the complaint, notify, in writing, the individual who made the complaint of his decision in relation to it so that the individual may, where he considers that he is aggrieved by the decision, appeal against it under section 51.

…

the Commissioner shall regulate the handling of complaints, investigations and conduct of hearings in such manner as he may determine."

1. The complaint process

Complaint is the process where data controllers or data subjects have the opportunity to exercise their rights under the Data Protection Act. The outline process is explained using the following flowchart.



2. How long does the complaint takes?

Depending on the complexity of the cases, it may take 3 months to one year or more. It also depends on collaboration of all parties and availability/gathering of evidences.

3. What is the result of the complaint?

It can be one of the following:

- an amicable resolution between the parties concerned.
- an offence being filed at the Office of the Director of Public Prosecution where the latter will decide if the offence has to be tried or not before a court.

4. Is the Decision of the Commissioner appealable?

Yes, it is appealable at the ICT Appeal Tribunal set up under section 35 of the Information and Communication Technologies Act.

Complaints (Process of Complaints)

Main Points	To do list
Complaint is a means to seek redress for the data subject from the controller or processor.	File the complaint on the appropriate form. Submit the statement form duly signed.
There can be amicable resolution or an offence being tried with the consent of the Director of Public Prosecution	
The decision of the Commissioner is appealable at the ICT appeal Tribunal.	Respond to all queries from the Data Protection Office.

EXCEPTIONS

What you need to know on the types of processing of personal data which are exempted from this Act (sections 3(4) and 44)?

Section 3(4)

"…

This Act shall not apply to –

(a) the exchange of information between Ministries, Government departments and public sector agencies where such exchange is required on a need-to-know basis;

(b) the processing of personal data by an individual in the course of a purely personal or household activity.

Section (44)

No exception to this Act shall be allowed except where it constitutes a necessary and proportionate measure in a democratic society for –

(a) subject to subsection (4), the protection of national security, defence or public security;
(b) the prevention, investigation, detection or prosecution of an offence, including the execution of a penalty;
(c) an objective of general public interest, including an economic or financial interest of the State;
(d) the protection of judicial independence and judicial proceedings; or
(e) the protection of a data subject or the rights and freedoms of others.

(2) The processing of personal data for the purpose of historical, statistical or scientific research may be exempt from the provisions of this Act where the security and organisational measures specified in section 31 are implemented to protect the rights and freedoms of data subjects involved.

(3) Where this section has been breached, a data subject or the Commissioner may apply for a Judge's order to protect the rights of individuals.

(4) (a) Personal data shall be exempt from any provision of this Act where the non-application of such provision would, in the opinion of the Prime Minister, be required for the purpose of safeguarding national security, defence or public security.

(b) In any proceedings in which the non-application of any provision of this Act on grounds of national security, defence or public security is in question, a certificate under the hand of the Prime Minister certifying that the non-application of the provision is required for the purpose of safeguarding national security, defence or public security shall be conclusive evidence of that fact."

1. Which type of processing personal data are exempted from the Data Protection Act?

In general, processing of personal data constitutes a necessary and proportionate measure in a democratic society for the following reasons:-

- the protection of national security, defence or public security
- the prevention, investigation, detection or prosecution of an offence, including the execution of a penalty
- an objective of general public interest, including an economic or financial interest of the State
- the protection of judicial independence and judicial proceedings
- the protection of a data subject or the rights and freedoms of others.

2. Are there other situations where exceptions are allowed?

The processing of personal data for the purpose of historical, statistical or scientific research is exempted provided that the security and organisational measures are implemented to protect the rights and freedoms of data subjects involved. The controller or processor has a duty to secure the data to prevent its unlawful disclosure.

3. How to secure the data as mentioned in 2 above?

The appropriate technology has to be used such as pseudonymisation or encryption.

4. Is personal data for domestic purposes exempted under this act?

Yes, the processing of personal data by an individual in the course of a purely personal or household activity is exempted.

A person has a list of contact numbers in 4 of his personal devices such as smartphone, tablet, desk computer and laptop which he uses for his household personal activity. This processing is exempted from the purview of the Data Protection Act.

5. Is personal data processed by Ministries and Government exempted under this Act?

Yes, it is exempted to ease the burden cast on citizens. Therefore, the exchange of information between Ministries, Government departments and public sector agencies where such exchange is required on a need to know basis is exempt under this Act.

OFFENCES AND PENALTIES

What you need to know on offences and penalties under the Data Protection Act?

There are various offences and criminal penalties under this Act which, in general if committed, is sanctioned by a court of law. They are listed in the following tables:

Offences	Penalties
Section 6: Investigation of Complaints Any person who fails to attend a hearing or to produce a document or other material when required to do so.	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.
Section 7: Power to require information Any person who fails or refuses to comply with a requirement specified in a notice, or who furnishes to the Commissioner any information which he knows to be false or misleading in a material particular	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.

Section 9: Enforcement notice Any person who fails or refuses to comply with an enforcement notice of the Commissioner	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.
Section 12: Obstruction of Commissioner or authorised officer Any person who obstructs or impedes the Commissioner or an authorised officer in the exercise of the power of entry and search or fails to provide assistance or information requested by the Commissioner or authorised officer or refuses to allow the Commissioner or an authorised officer to enter any premises or to take any person with him in the exercise of his functions.	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.
Section 15: Application for registration Any controller or processor who knowingly supplies any information, during registration, which is false or misleading in a material particular	Liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.
Section 17: Change in particulars Any controller or processor who fails to notify a change in particulars	Liable to a fine not exceeding 50, 000 rupees.
Section 28: Lawful processing Any person who process personal data unlawfully	Liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.

Section 29: Special categories of personal data Any person who processes special categories of data unlawfully	Liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.
Section 43: Offence for which no specific penalty provided Any person who commits an offence under this Act for which no specific penalty is provided or who otherwise contravenes this Act	Liable to a fine not exceeding 200, 000 rupees and to imprisonment for a term not exceeding 5 years. A Court may also order the forfeiture of any equipment or any article used or connected in any way with the commission of an offence or order or prohibit the doing of any act to stop a continuing contravention.
Section 49: Confidentiality and oath Any person who, without lawful excuse divulge any confidential information obtained in the exercise of a power or in the performance of a duty under this Act	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years. Protection from liability also applies.