Guide on National Security and Privacy

DPO
Data Protection Office

Table of Contents

List of Abbreviations

CJEU	Court of Justice of the European Union
DPA	Data Protection Act 2017
DPIA	Data Protection Impact Assessment
DPO	Data Protection Office
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
GDPR	General Data Protection Regulation
UK DPA 2018	UK Data Protection Act 2018

1. Definitions

Data Subject

An identified or identifiable individual (any data which can identify an 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.

Personal Data

Any information relating to a data subject.

Special Categories of Personal Data

Personal data of the data subject pertaining to his racial or ethnic origin; his political opinion or adherence; his religious or philosophical beliefs; his membership of a trade union; his physical or mental health or condition; his sexual orientation, practices or preferences; his genetic data or biometric data uniquely identifying him; the commission or alleged commission of an offence by him, 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 such other personal data as the Commissioner may determine to be sensitive personal data.

Controller

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

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

Processing

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.

2. Introduction

Many countries implement different types of projects in the interest of national security, defence and public security to ensure that state authorities can better protect the citizens they serve. Whilst new technologies are powerful, they can also be dangerous if they are misused or fall in the wrong hands. For example, Edward Snowden's revelations in 2013 regarding the operations of massive internet and phone surveillance programmes by US intelligence agencies have ignited serious concerns on the dangers that such surveillance activities can have on privacy, democratic governance and freedom of expression.

Citizens and the media have very often questioned the adequacy of national security projects on human rights' aspects. For instance, some countries may not have an adequate legal framework to regulate national security systems, whilst sometimes, the law itself does not provide enough precision on measures for addressing national security projects . As a consequence, citizens tend to be confused on the legal basis and reasons for which such surveillance activities are carried out. In the case of Digital Rights Ireland Ltd versus Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others in April 2014, an assessment of the EU Directive 2006/24 was carried out. This Directive requested telephone communications service providers to retain traffic and location data of the users of these providers for a period specified by law to prevent, detect, investigate and prosecute crime and safeguard national security within the EU. The CJEU held that this Directive was in breach of the fundamental rights of private life and the protection of personal data respectively and thereby invalidated the Directive 2006/24 because it would constitute an interference with the electronic communications of practically the entire european population.

In this perspective, an effective operation and supervision of national security projects are important to ensure that fundamental rights such as privacy are not compromised. Hence, the purpose of this guide is to examine the privacy implications of national security projects including particularly the provisions on national security in the DPA. The guide also sets out several recommendations to controllers and processors on the adoption of recommended privacy compliance practices for national security projects.

This guide is intended solely for those organisations which can demonstrate that national security is part of their functions as attributed by law.

3. Privacy risks of national security projects

Generally, the "privacy of an individual is the right to be let alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used"[1].

National security projects very often involve the processing of huge amounts of personal data of individuals. The processing activities may include any type of operations on the data such as

the interception, collection, transmission, use, storage or transfer, amongst others. Privacy concerns generally arise with respect to the wide range of activities that may be performed on the data. Sometimes, the processing of operations may involve special categories of personal data, which would require enhanced protection, due to their sensitive nature and increased privacy risks. An example of special categories of personal data is biometric data.

The scope of surveillance for national security interests is constantly evolving as new technologies emerge. Initially, surveillance was carried out on a specific individual or on an organisation such as tapping his/her telephone on grounds of reasonable suspicion that the latter was involved in criminal activities or represented a danger for national security[2]. With advancements in technology, surveillance may now be carried out by powerful tools indiscriminately and continually resulting in the automatic collection of bulk personal data, which might afterwards be analysed for persons/organisations of interests to national security agencies. This method has triggered significant privacy implications on the impact and potential use of bulk data processed. Moreover, surveillance can also be done remotely using communication network exploitation techniques to extract information within computers by injecting malware on computer systems.

Although privacy is not an absolute right and can be lawfully constrained for national security purposes, when satisfying necessity and proportionate measures, the right to privacy still remains a fundamental human right. Controllers implementing projects of national security interests must adopt the right approach to avoid any undue harm to any citizen in view of the privacy risks that such projects may entail.

4. An international perspective of legal frameworks on national security

Many countries have set up different legal regimes when addressing national security concerns to preserve public security against terrorist activities and for other legitimate purpose(s).

An analysis of different jurisdictions namely the United States (US), Europe and the United Kingdom (UK) is set out below to provide a brief overview of the diversity of legal systems on national security and privacy provisions.

US

- In general, the US has several sector-specific national privacy or data security laws that are scattered in a whole panoply of statutes. However, the central legislation targeting national security is the 1947 National Security Act.

- It is to be noted that international human rights law provides a universal framework against which any interference within individual privacy rights must be assessed. It is codified in the United Nations' (UN) Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights. Article 12 of the Declaration and Article 17 of the International Covenant declare that no one shall be subjected to arbitrary or unlawful interference with his privacy on matters of national intelligence[3].

- The UN General Assembly resolution 68/167 of January 2014 emphasized the importance of finding the right balance between privacy and security. In this regard, it was stipulated that "public security may justify the gathering and protection of certain sensitive information, but States must ensure full compliance with their obligations under international human rights law." [4]

- The UN Report on the Right to Privacy in the Digital Age underlined in its recommendations and conclusions that "there is a clear and pressing need for vigilance in ensuring the compliance of any surveillance policy or practice with international human rights law, including the right to privacy, through the development of effective safeguards against abuses"[5]. The report deplored the circumstances in many countries which have contributed to a lack of accountability for arbitrary or unlawful interference within the right to privacy.[3]

Europe

i. European Convention on Human Rights (ECHR)

Article 8 (2) of ECHR specifies that interference by a public authority with regard to the right to respect for private life can only be admissible if such restriction is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

ii. General Data Protection Regulation (GDPR)

The GDPR specifies in Article 23 that the Union or Member State law by way of legislative measure may restrict the scope of certain obligations and rights. Some of these include the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling (Articles 12 to 22), as well as the communication of a personal data breach to a data subject (Article 34) and certain related obligations of the controllers (such as Article 5), as far as they are necessary and proportionate in a democratic society to safeguard national security, defence, public security, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties.

iii. Council of Europe

The practical guide on the use of personal data in the police sector

This guide provides in Point 7 exceptions from the application of data protection principles concerning national security, defence, public safety, important economic and financial interests. It also stipulates that "exceptions would have to be incorporated into national legislation and should not be described in a general way, but should serve a well-defined purpose"[6].

The exceptions that may be applicable are the collection of data and use of data, subsequent use of data, processing of special categories of personal data, providing information to data subjects as well as to the data subjects' rights.

Modernised Convention for the protection of individuals with regard to the processing of personal data (Convention 108 +)

Article 11 of the Convention stipulates that no exemptions to the provision set out

in this part shall be allowed except for the provisions of Article 5(4) on the principles relating to the processing of personal data, Article 7(2) on the communication of personal data breach to a supervisory authority, Article 8(1) on the transparency of processing – Information to be provided to the data subjects before collecting/processing personal data and Article 9 on the rights of the data subject when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms, and constitutes a necessary and proportionate measure in a democratic society for the protection of national security, defence, public safety, important economic and financial interests of the State, the impartiality and independence of the Judiciary.

Furthermore, Article 11(3) of the Convention stipulates that in addition to the exceptions allowed for in Article 11(1) of this article, with reference to processing activities for national security and defense purposes, each Party may provide, by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim, exceptions to Article 4(3), Article 14 (5)and (6) and Article 15(2)(a)(b)(c) and (d).

It is thus observed that no complete exemption is provided for national security as specified in Article 11 of the Convention.

Case Law

In Roman Zakharov v. Russia No. 47143/06, the applicant sued three mobile network operators, deploring that the right to privacy of his telephone communications had been breached. This is due to the fact that the operators had installed equipment, enabling the Federal Security Service to intercept his telephone communications without prior judicial authorisation.

In its ruling, the ECtHR established that there had been a breach of Article 8 of the European Convention of Human Rights (Right to respect for private and family life, home and correspondence). This was due to the fact that the legal regime on interception of communications failed to cater for adequate and effective safeguards to prevent the risk of abuse from the part of secret services and police.

The UK Data Protection Act 2018

The UK DPA 2018 sets out the data protection framework in the UK, alongside the GDPR. The UK DPA 2018 provides an exemption from particular GDPR provisions. If an exemption applies, an organisation may not have to comply with all the usual rights and obligations. Besides, the 2018 Act creates a new framework for data processing, catering for a separate regime to govern the processing of personal data by the intelligence services.

Section 26 of the UK DPA 2018 provides an exemption from the provisions of the Act (including data protection principles except for lawful, fair and transparent processing, rights of data subjects, notification and communication of personal data breaches, amongst others) if the exemption from the provision is necessary for safeguarding national security or defence purposes.

Part 4 of the Act introduces a data protection regime applicable to the processing of personal data by intelligence services. This part provides a specific regime for intelligence services, which makes sure that the processing of personal data by these agencies is subject to appropriate and proportionate controls. The UK DPA 2018 caters for the following:

- Section 110 provides that the intelligence services can be exempted from the specified provisions of the regulatory scheme where it is necessary to safeguard national security (the 2018 Act also provides for other exemptions for the intelligence services in Schedule 11).

- Section 111 provides that a certificate, signed by a Cabinet Minister (or the Attorney General or the Advocate General for Scotland) is conclusive evidence that an exemption relied upon by the intelligence services from any or all of the specified data protection requirements is required to safeguard national security which is similar to section 44 (4) of the DPA.

Case Law

In the case of Kennedy v. The United Kingdom 26839/05 [2010] ECHR 682, the claimant alleged that he had been under secret surveillance. Yet, he contended that he did not have any access to certain confidential data held by national authorities on him.

The court held that his request to gain access to his confidential data did not constitute any breach of Article 8 of the ECHR. This is because under secret surveillance measures, there was a need to preserve secret sensitive and confidential information to the extent that they were strictly necessary for the safeguard of democratic institutions.

In light of the diverse international frameworks described above, it is observed that generally **no absolute** exemption is provided for national security and defence purpose(s). In case a national security project requires certain restrictions from privacy laws, then appropriate legislative measures must be enacted where it is considered as necessary and proportionate to do so.

In addition, if the GDPR and the UK DPA 2018 are considered, the practice seems to be that States do not allow for exemptions pertaining to the provision on lawfulness of processing even if it is for national security or defence purposes. It is thus primordial that any intelligence service or other controller who is processing personal data for this purpose identify its lawful basis for processing at the very start of the project.

Controllers and processors are also required to comply with other provisions of data protection/ privacy laws which have not been exempted. For instance, controllers and processors are always required to put in place appropriate technical and organisational measures when processing personal data for national security and defence purposes.

5. Data Protection Act 2017

The DPA in Mauritius safeguards the privacy rights of individuals. The DPO is the national supervisory authority for enforcing the provisions of the DPA. The office acts with complete independence and impartiality in the discharge of its functions under section 4 of the DPA.

The DPA also provides a wide range of powers to the Data Protection Commissioner in carrying out the functions and enforcing the provisions of the Act such as the power to require information, preservation order, enforcement notice, power to seek assistance, power of entry and search, delegation of power by Data Protection Commissioner, prior security check and compliance audit.

All controllers and processors operating in Mauritius must comply with the provisions of the DPA. Emphasis is being laid on sections 28, 29 and 31 of the DPA which underpin the implementation of any project.

5.1. Lawful Basis for Processing

There are several legal basis for the processing of personal data under section 28 of the DPA and stricter conditions permitting the processing of special categories of personal data, such as health data, under section 29 of the DPA.

The consent of an individual is not the only legal ground that allows for the lawful processing of

personal data. If an organisation satisfies any other legal basis provided under the DPA apart from consent, the processing will be considered as being lawful.

Section 28 - Lawful processing

(1) 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

(2) Any person who contravenes subsection (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.

Under the DPA, controllers and/or processors must implement enhanced protection when processing special categories of personal data. There are also a limited number of conditions that allow for the lawful processing of these data. A controller is required to satisfy both a lawful basis under section 28 of the DPA and a separate condition for processing special categories of personal data under section 29.

Section 29 - Special categories of personal data

(1) Special categories of personal data shall not be processed unless –

(a) section 28 applies to the processing; **and**

(b) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body

with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(c) the processing relates to personal data which are manifestly made public by the data subject; or

(d) the processing is necessary for –

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

(ii) the purpose of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to a contract with a health professional and subject to the conditions and safeguards referred to in subsection (2);

(iii) the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; or

(iv) protecting the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.

(2) The personal data referred to in subsection (1) may be processed for the purposes referred to in subsection (1)(d)(ii) where the data are processed by or under the responsibility of a professional or other person subject to the obligation of professional secrecy under any enactment.

(3) Any person who contravenes subsection (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.

5.2. Security of Processing

A key requirement of the DPA is that a controller or processor must process personal data securely by means of appropriate technical and organisational measures.

According to section 31 of the DPA, the measures shall include -

i. the pseudonymisation and encryption of personal data;
ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
iii. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
iv. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Confidentiality, Integrity and Availability (CIA) are the three key elements of information security.

If any of the three elements is compromised, this can lead to serious consequences for both the controller as well as individuals whose data are processed. A controller must seek to guarantee the three elements of the CIA at all times in both systems and data.

A list of non-exhaustive safeguards to promote the security of data is provided in Annex I of this guide.

6. Exceptions and restrictions

Section 44 of the DPA enumerates the circumstances where privacy rights may be restricted.

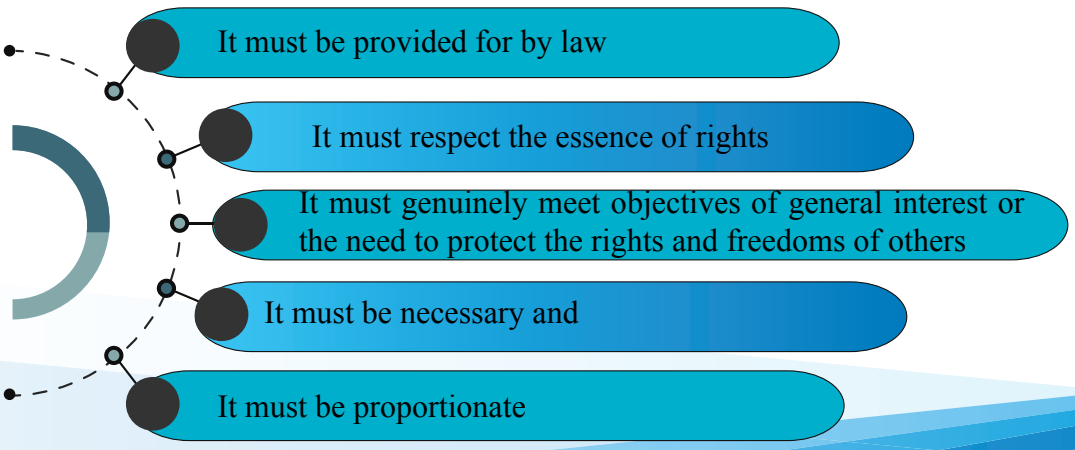
Section 44 - Exceptions and restrictions

(1) 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;
- (e) the protection of a data subject or the rights and freedoms of others; or
- (f) issue of any licence, permit or authorisation during the COVID-19 period. (Amended by the Covid-19 (Miscellaneous Provisions) Act 2020)

(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.

Moreover, any limitation(s) or restriction(s) on the exercise of rights protected under the DPA 2017 must be lawful and comply with the following criteria:



Thus, for projects where restrictions of the provision(s) of the DPA 2017 are envisaged, specific legislation should be enacted or existing legislation should be amended by the controller to meet the legality assessment of the proposed processing.

For example, the National Identity Card (Miscellaneous Provisions) Act 2013 was amended to introduce a new smart identity card, which incorporates on a chip the citizen's fingerprints and other biometric information relating to his or her external characteristics. Following the Supreme Court judgement in the case Madhewoo M. v the State of Mauritius and Anor and Jugnauth Pravind Kumar (Hon) v the State of Mauritius & Anor [2015] SCJ 178, the Act was subsequently amended to delete fingerprint data after the card had been issued to the cardholder.

6.1. National security, defence or public security

When projects relate to national security, defence or public security purpose(s), then under section 44(4)(b), a certificate may be issued 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. The certificate will be considered as conclusive evidence of same.

(44) (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.

The onus is on the controller to decide on which section(s) of the DPA it would require an exception for the relevant certificate. In general, any controller must comply with all the relevant provisions of the DPA as listed in the table below.

Provision of DPA	Description	Implication
Part II Functions and Powers of the Commissioner (Sections 6 - 12)	Provide powers to the Data Protection Commissioner for the following: 1. Investigation of complaints 2. Power to require information 3. Preservation order 4. Enforcement notice 5. Power to seek assistance 6. Power of entry and search 7. Obstruction of Commissioner or authorised officer.	The Data Protection Commissioner may exercise her powers with respect to processing of personal data for a given project.
Part III Registration and renewal as controller and processor (Sections 14 -18)	All controllers and processors must register and renew their registrations with the Data Protection Commissioner.	A controller must register with the DPO and update its registration with respect to personal data processed under the project. If the service of a processor is sought in the implementation of the project, the procesor must also register and renew its applications with the office.
Part IV - Obligations of controllers and processors		
Principles for processing personal data (Section 21)	The following 6 principles of processing must be complied with: 1. Lawful, fair and transparent; 2. Purpose limitation; 3. Data minimisation; 4. Data accuracy; 5. Storage limitation; 6. In accordance with the rights of data subjects.	A controller must ensure that the processing of personal data under the project meets these six principles.

Duties of controller (Section 22)	Implement appropriate data security and organisational measures (section 31); Keep a record of all processing operations (section 33); Perform a Data Protection Impact Assessment (section 34); Comply with the requirements for prior authorisation from, or consultation with the Commissioner (section 35); Designate a Data Protection Officer responsible for data protection compliance; Verify the effectiveness of measures implemented.	A controller must fulfill all its duties under the DPA.
Collection of personal data (Section 23)	Collect personal data for a lawful purpose and only if it is necessary. Provide data subjects with all information described under section 23(2) such as the purpose(s) for processing their personal data, retention period for the personal data, and who it will be shared with, amongst others.	A controller must inform data subjects of all information regarding the collection of personal data for a project.
Conditions for consent (Section 24)	A controller must bear the burden of proof for establishing consent; An individual must be able to withdraw his consent at any time; Consent is presumed not to be freely-given if the performance of a contract/service is dependent on the consent which is not necessary for the execution of the contract/service.	A controller must fulfill all the conditions for consent if consent is being sought as the lawful ground for processing personal data for the project.

Notification of personal data breach (Section 25)	Notify a personal data breach to the DPO where feasible not later than 72 hours after becoming aware of it. The relevant notification form is available on the website of the DPO.	A controller must notify the office on any personal data breach under the project. Any processor acting on behalf of a controller must inform the latter of any personal data breach without undue delay.
Communication of breach to data subject (Section 26)	Inform data subject of breach, where it is likely to result in a high risk to the rights and freedoms of the data subject.	A controller must communicate a personal data breach to data subjects if it is likely to result in a high risk to their rights and freedom.
Duty to destroy personal data (Section 27)	Destroy personal data as soon as is reasonably practicable when the purpose has lapsed, and notify any processor holding the data for destruction.	A controller must destroy the personal data when the purpose for holding it lapses.
Lawful processing (Section 28)	Comply with at least one criterion for lawful processing.	The processing of personal data for a project must comply with at least one lawful basis for processing.
Special Categories of personal data (Section 29)	Implement specific protection and a stricter regime.	A controller must ensure compliance with section 29 when special categories of personal data are processed.
Security of processing (Section 31)	Implement appropriate security and organisational measures.	A controller must put in place appropriate measures to ensure security of personal data. If a controller uses the services of a processor, it must ensure through a written contract with the processor that the latter acts only on its instructions and undertakes appropriate security measures.

Record of processing operations (Section 33)	Maintain a record of all processing operations. The template is available on DPO website.	A controller must document all processing activities under the project.
Part V- Processing operations likely to present risk		
Data Protection Impact Assessment - DPIA (Section 34)	Perform a DPIA. Guidance on how to evaluate high risk processing operations and DPIA form is available on DPO website. Comply with the requirements for prior authorisation from, or consultation with the Commissioner.	For high risk processing operations, the controller must carry out a DPIA prior to the processing.
Part VI - Transfer of personal data outside Mauritius		
Transfer of personal data outside Mauritius (Section 36)	If a controller or processor cannot provide proof of appropriate safeguards or cannot rely on any of the exceptions provided in section 36(1):-{Consent from individual, Contract with individual, Public interest, Legal claim, Vital interest and Legitimate interest}, then authorisation from the Data Protection Commissioner is required for the transfer.	A controller must satisfy section 36 in case personal data is transferred outside Mauritius.

Part VII - Rights of Data Subjects		
Rights of Data Subjects (Sections 37 –41)	Right of access; Right not to be subject to automated decision making including profiling; Right to rectification, erasure or restriction of processing; Right to object; Exercise of rights.	A controller must provide these rights to data subjects.
Part VIII - Other offences and penalties		
Unlawful disclosure of personal data (Section 42)	Unlawful disclosure of personal data	A controller must ensure that there is no unlawful disclosure of personal data under the project.
Part IX Miscellaneous		
Compliance audit (Section 46)	Compliance audit	The Data Protection Commissioner may carry out periodical compliance audits.

In principle, any limitation or restriction to the provisions of the DPA as provided above should meet the tests of necessity and proportionality in a democratic society as stipulated under section 44(1) of the DPA and be provided by law.

The controller should stand guided by the State Law Office on the drafting of the certificate under sections 44 (4)(a)&(b) and notify the DPO accordingly.

7. Necessity and proportionality principles in a democratic society

This section aims to assist policymakers in finding solutions which will minimise the risk of having conflicting priorities/objectives with privacy and data protection considerations.
The UN High Commissioner for Human Rights highlighted the importance of the necessity and proportionality principles as follows:

"It will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate."(UNHCHR 2014: §25)

7.1. Checklist for assessing the necessity and proportionality of national security projects

Necessity

Necessity requires a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive in comparison with other options to attain the same goal.[10]

Test for necessity

The diagram below shows a series of steps that can be followed in order to ensure that any national security project complies with the necessity principle in relation to the objective(s) pursued.

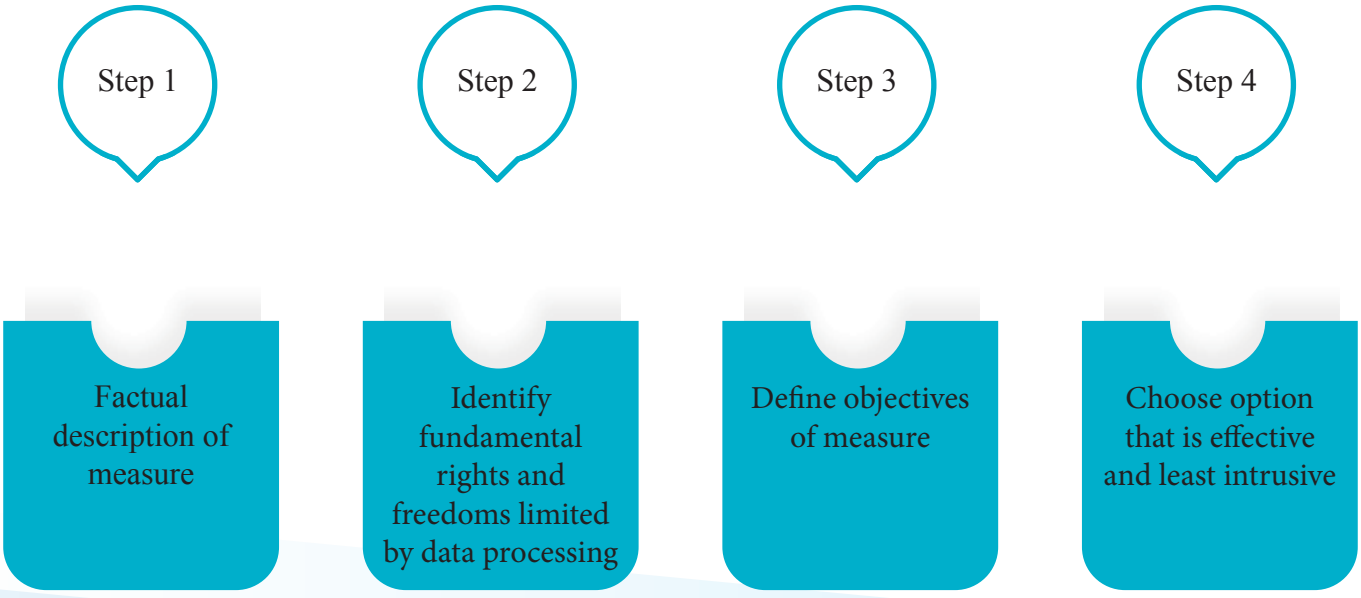


Diagram from EDPS (2017)[10]

A controller cannot proceed to the test of proportionality if the test of necessity fails.

Proportionality

Proportionality is a general EU law principle which "restricts the authorities in the exercise of their powers by requiring a balance to be struck between the means used and the intended aim (or result reached)". [11]

Test for proportionality

The diagram below provides the steps to be considered when determining whether any measure adopted for a national security project will be proportionate in relation to the objective(s) pursued.

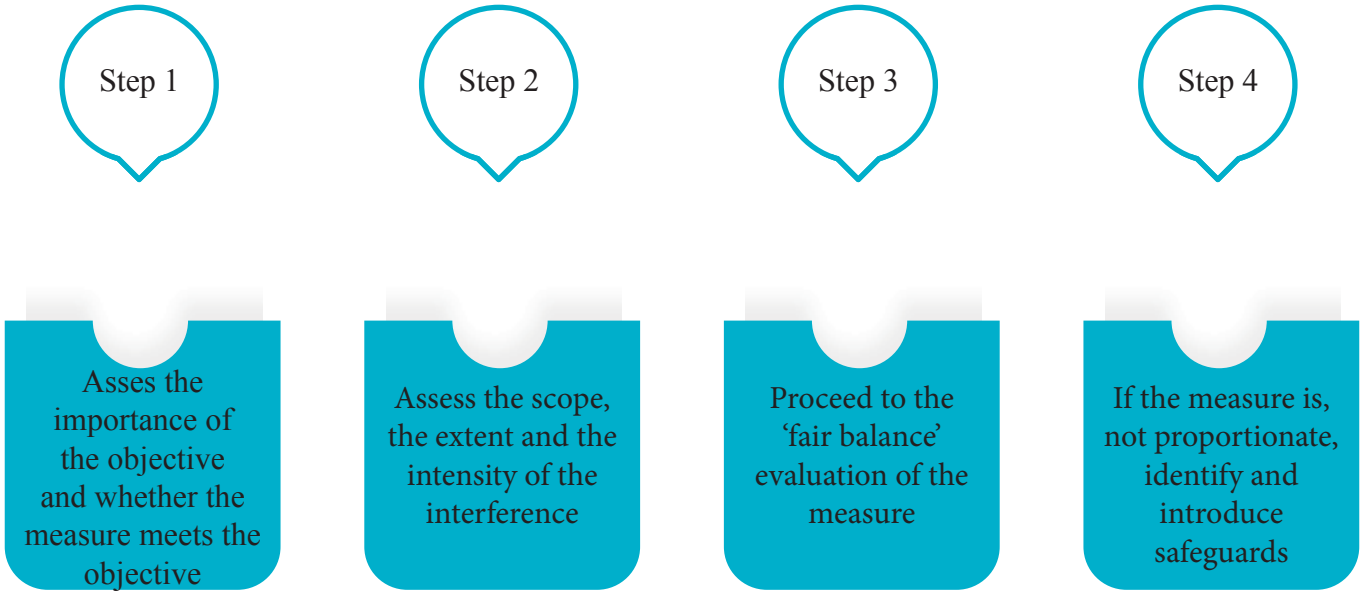


Diagram from EDPS (2019)[11]

The following case illustrates the application of the principle of proportionality:-

Ministerio Fiscal (CJEU, C-207/16, ECLI:EU:C:2018:788)

As part of a robbery, a mobile phone was lost. Consequently, during the investigation process, the police had requested the investigating Magistrate to order various providers of electronic communications services to provide (i) the telephone numbers that had been activated for a specified period of time with the International Mobile Equipment Identity code ('the IMEI code') of the stolen mobile telephone and (ii) the personal data relating to the identity of the owners or users of the telephone numbers corresponding to the SIM cards activated with the code, such as their surnames, forenames and, if need be, addresses.

The request for accessing such data was pertinent to the investigation since the SIM card(s) activated with the stolen mobile telephone could be linked, during a specific period, with the identity

of the owners of those SIM cards. Without those data being cross-checked with the data pertaining to the communications with those SIM cards and the location data, those data would not render it possible to ascertain the date, time, duration and recipients of the communications made with the SIM card or cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period.

In relation to the request made for accessing such data, the CJEU held that owing to the fact that these data did not allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned, the interference was not considered to be sufficiently serious to restrict access to the personal data of potential criminals.

The CJEU has also ruled out that when the crime is 'serious', then a serious interference to access the personal data in question can be justified in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime.

8. Privacy by design

Privacy by design is a recommended approach to projects to promote privacy and data protection compliance from the start. A project may fail if it has not been planned correctly. Controllers must therefore ensure that privacy considerations are identified from the early stages of project and sufficient analysis is undertaken by a controller to identify solutions on the market that use a privacy by design concept.

9. Data Protection Impact Assessment

According to section 34 of the DPA, a DPIA has to be carried out by the owner of the project to assess the necessity and proportionality of the processing operations and purposes. The DPIA will also ensure that the risks to the rights and freedoms of individuals have been mitigated and that the security of personal data has been addressed adequately.

Under section 34 (2) of the DPA, a DPIA must be carried out where the processing operations involve :

(a) a systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or significantly affect the individual;

(b) processing on a large scale of special categories of data referred to in section 29;

(c) a systematic monitoring of a publicly accessible area on a large scale;
(d) any other processing operations for which consultation with the DPO is required.

Furthermore, as per section 34 (3), the assessment must include :

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller or processor;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects;
(d) the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights and legitimate interests of data subjects and other persons concerned.

Section 34 (4) specifies that the controller or processor must seek the views of data subjects on the intended processing where appropriate, without prejudice to the protection of commercial or public interests or the security of the processing operations.

A DPIA should be started as early as practicable in the design of the processing operation. The DPIA can be updated throughout the different phases of the project.

The responsibility of conducting a DPIA lies on the controller. However, if the processing is wholly or partly performed by a processor, the latter may also assist the controller in carrying out the DPIA in providing any necessary information. The DPIA form is available on the website of the Data Protection Office.

The DPO has published on its website at the following URL: http://dataprotection.govmu.org/English/Pages/Data-Protection-Impact-Assessment-and-High-Risk-Operations.aspx a list of criteria evaluating high-risk processing operations.

10. Checklist for projects of national security interests

SN	Details
1.	Who will act as controller and be responsible for the processing of the personal data under the DPA?
2.	Is there any processor or subcontractor involved in this project? If yes, (a) Are they bound by a contract? (b) How do you ensure that there is an adequate level of security in place?
3.	Is the controller/processor registered with the DPO as per section 14 of the DPA?
4.	Have you nominated a data protection officer as per section 22(2)(e) of the DPA?
5.	What is the purpose of the project?
6.	What types of personal data will be processed for this project?
7.	Does the project involve the processing of special categories of personal data that merit enhanced protection under the DPA (e.g. health data, criminal offences, biometric data amongst others)?
8.	Does the project involve processing of personal data of children below age of 16?
9.	Will you rely on section 28 or section 44 of the DPA? If so, please provide more details.
10.	Are you seeking any exceptions and restrictions from any provisions of the DPA? Please provide details.
11.	Have you consulted the State Law Office for advice?

12.	Does the project require any enactment/amendment of any legislation or regulation to allow for the processing of personal data?
13.	Have you conducted the necessity and proportionality tests when designing the project?
14.	Do you limit the collection of personal data, to only those items that are necessary and ensure they are not used in any manner incompatible with these purposes?
15.	Will personal data be exchanged between Ministries, Government departments and public sector agencies where such exchange is required on a need-to-know basis? If so, please provide details.
16.	Have you established procedures for notification of personal data breaches to the DPO as per section 25 of the DPA?
17.	Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, do you plan to inform the concerned individuals as per section 26 of the DPA?
18.	Are there countries where such types of projects have been implemented?
19.	Are there specific legal frameworks that have been established in those countries to allow the operation of such projects?
20.	Have you conducted a research on the privacy implications of such types of projects in countries where similar projects have been implemented?
21.	Have you conducted and submitted the Data Protection Impact Assessment to the DPO in accordance with section 34 of the DPA?
22.	What are the organisational and technical measures that will be implemented to ensure the security of the personal data processed as per section 31 of the DPA?
23.	Are procedures in place to ensure that all data that will be collected are accurate, complete, and up-to-date?

24.	Do you have defined rules and procedures governing the use and disclosure of personal data?
25.	What is the retention time for keeping personal data processed for the project?
26.	What will happen to these data after the retention period expires? Will the data be erased or anonymised?
27.	Are you keeping a record for the processing of operations in accordance with section 33 of the DPA?
28.	Will data be transferred outside Mauritius? If so, please specify the relevant section under section 36(1) of the DPA for the transfer.
29.	Are your staff sufficiently trained to process data under this project?

11. Conclusion

National security, defence and public security exemptions should not routinely be relied upon in general ways or applied in a blanket fashion. They should be considered on a case-by-case basis for each project after taking into consideration all privacy and data protection implications. In line with the principle of accountability, a controller should be in a position to justify and document the reason(s) for relying on the national security, defence and public security exemption so that it can demonstrate its compliance with the DPA.

12. References

1. IAPP, 2020, What does privacy mean? - https://iapp.org/about/what-is-privacy/(last visited on 12.02.2020)
2. Democratic and effective oversight of national security services by the Council of Europe - https://rm.coe.int/1680487770 (last visited on 22.05.2020)
3. WP228- Working Document on surveillance of electronic communications for intelligence and national security purposes - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf (last visited on 22.05.2020)
4. UN General Assembly resolution 68/167, 21 January 2014 – http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167 (last visited on 07.04.2020)
5. Report of the UN High Commissioner for Human Rights on the right to privacy in the digital age. Distributed 30 June 2014. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (last visited on 07.04.2020)
6. Practical guide on the use of personal data in the police sector - https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5 (last visited on 02.05.2020)
7. The European Union General Data Protection Regulation (GDPR) - https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504 (last visited on 22.05.2020)
8. Convention 108 + - Convention for the protection of individuals with regard to the processing of personal data - https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (last visited on 01.05.2020)
9. Data Protection Act 2018 Factsheet – Intelligence services processing (Sections 82 - 113) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711233/2018-05-23_Factsheet_4_-_intelligence_services_processing.pdf (last visited on 01.05.2020))
10. European Data Protection Supervisor (2017), 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf (last visited on 21.05.2020)
11. European Data Protection Supervisor (2019),'EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data'https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf (last visited on 10.04.2020)

13. Annex

Some non-exhaustive safeguards to promote the security of personal data

a. Implementation of physical safeguards to limit physical access to sensitive information, systems, related facilities, and equipment from unauthorized access as well as natural and environmental hazards.
b. Implementation of technical and organisational measures (e.g. privacy policy, information security policy, amongst others) to protect data.
c. Conducting risk-based audit programs to ensure effectiveness of data security policies and procedures.
d. Implementation of information security awareness and training programmes for providing employees with the information and tools needed to protect the organization's information assets.
e. Implementation of access controls to ensure that user access rights reflect defined and documented business needs and job requirements.
f. Development of practices that will help to reduce the risk of insider attacks such as segregation and rotation of duties, least privilege, log monitoring and administrative account control.
g. Regular testing of key controls, systems and procedures to obtain assurance and confidence that the security implemented controls are operational and effective in their application.
h. Logging and monitoring of activities to assess policy compliance, identify intrusions and breaches.
i. Development of formal change management procedures covering both normal and emergency changes to systems processing sensitive information.
j. Evaluation of all transfers of physical media containing sensitive information.
k. Encryption of data in transmission and storage.
l. Implementation of an e-mail acceptable use policy and to clearly describe applicable restrictions on the transmission of sensitive information via e-mail.
m. Encourage the use of privacy enhancement technologies to protect data.
n. Use of a variety of technical safeguards for data security, including firewalls, intrusion detection systems, penetration testing and vulnerability scanning.
o. Implementation of policies and processes governing the conditions under which remote access is granted and terminated.
p. Ensuring all remote communications are done through a virtual private network that can provide a secure communication channel.
q. Configuration of all servers and workstations with antivirus software that is automatically updated daily with new virus definitions.
r. Passwords adherence to complexity and ageing requirements.
s. Periodic assessments and reviews of entitlement privileges and permissions to systems and data.

t. Scheduled backups of data within a secured storage environment.

u. Strengthen controls of developers' access to controlled information systems and sensitive data.

v. Implementation of effective disaster recovery/business continuity planning (DR/BCP) to establish the basis for the organisation to maintain and recover business processes when operations have been disrupted unexpectedly.

w. Implementation of appropriate disposal practices and media sanitisation to prevent unauthorised access or use of the information.

Issued by the Data Protection Office

5th Floor, Sicom Tower, Wall Street, Ebene
http://dataprotection.govmu.org
dpo@govmu.org