



# DATA PROTECTION AND THE MEDIA



# **DATA PROTECTION AND THE MEDIA**

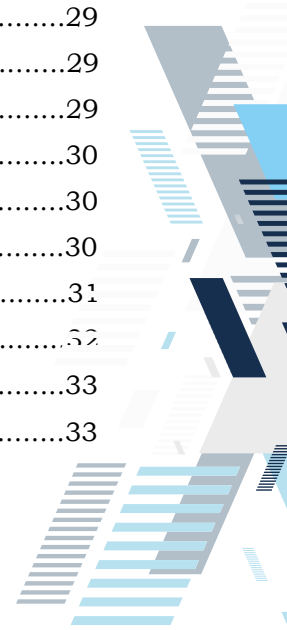
Data Protection Office





# TABLE OF CONTENTS

TERMS.....	1
1. INTRODUCTION.....	3
2. FREEDOM OF EXPRESSION, THE ROLE OF THE MEDIA AND RESPONSIBLE JOURNALISM.....	5
2.1. Freedom of expression.....	5
2.2. Media as public watchdogs with rights and responsibilities.....	6
2.3. Responsible journalism v. tabloid journalism.....	8
3. PRIVATE LIFE AND CONDITIONS FOR PUBLISHING PRIVATE MATTERS.....	9
3.1. Private life.....	9
3.2. Consent.....	9
3.3. Public interest .....	10
3.3.1. Public figures .....	12
3.3.2. Private individuals.....	14
3.4. Framework for balancing the rights to privacy and freedom of expression....	14
3.4.1. Contribution to a debate of general interest.....	14
3.4.2. The role of the person concerned and the subject of the report.....	16
3.4.3. Prior conduct of the person concerned.....	18
3.4.4. Method of obtaining information and its veracity.....	18
3.4.5. Content, form and consequences of publications.....	19
4. SPECIFIC ISSUES OF PRIVATE LIFE.....	21
4.1. Family, home, property.....	21
4.2. Physical and moral integrity.....	21
4.3. The right to one's image.....	22
4.3.1. Specific cases of photographing and filming.....	24
4.3.2. Correspondence.....	27
5. CRIME REPORTING.....	28
5.1. General principles.....	28
5.2. The right of victims (minors) to protect their identity.....	28
5.3. The right to privacy of a presumed pedophile.....	29
5.4. Revealing the identity of an investigated police officer.....	29
5.5. Suspected persons.....	29
5.6. Publishing banal aspects of accused persons.....	30
5.7. Persons in custody.....	30
5.8. Convicted persons in emotional situations.....	30
5.9. Convicted persons released on parole.....	31
6. CODES OF CONDUCT AND SELF-REGULATORY TOOLS.....	32
7. DATA PROTECTION PRINCIPLES.....	33
7.1. Functions of the Data Protection Office.....	33



7.2.	Powers of the Data Protection Office.....	34
7.2.1.	Power to require information.....	34
7.2.2.	Preservation order.....	35
7.2.3.	Enforcement notice.....	35
7.2.4.	Power to seek assistance.....	35
7.2.5.	Power of entry and search.....	35
7.2.6.	Delegation of power by Data Protection Commissioner.....	36
7.2.7.	Prior security check.....	36
7.2.8.	Compliance audit.....	37
7.3.	Registration.....	37
7.4.	Principles relating to processing of personal data.....	37
7.5.	Duties of controller.....	38
7.6.	Collection of personal data.....	38
7.7.	Conditions for consent.....	39
7.7.1.	Elements of a valid consent:.....	39
7.7.2.	Section 24 of the DPA.....	40
7.8.	Notification of personal data breach and Communication to the data subject..	41
7.9.	Duty to destroy personal data.....	43
7.10.	Lawful processing.....	43
7.11.	Special categories of personal data.....	43
7.12.	Personal data of child.....	44
7.13.	Security of processing.....	45
7.14.	Record of processing operations.....	47
7.15.	Data Protection Impact Assessment (DPIA).....	47
7.16.	Prior Authorisation and Consultation.....	49
7.17.	Transfer of personal data.....	50
7.18.	The rights of individuals.....	51
7.18.1.	Right of access.....	52
7.18.2.	Right of rectification, erasure or restriction.....	53
7.18.3.	Right to object.....	53
7.19.	Processing of non-editorial content.....	53
7.20.	Best practices to ensure and demonstrate compliance.....	55
8.	REFERENCES.....	56





## TERMS

### **Data Protection Act 2017 (DPA):**

The law which governs the protection of personal data in Mauritius.

### **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.

### **Data Subject (Individual):**

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.

### **Personal Data :**

Any information relating to a data subject.

 **Special categories of 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 of 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

#### ✦ 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.

#### ✦ 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.

# INTRODUCTION

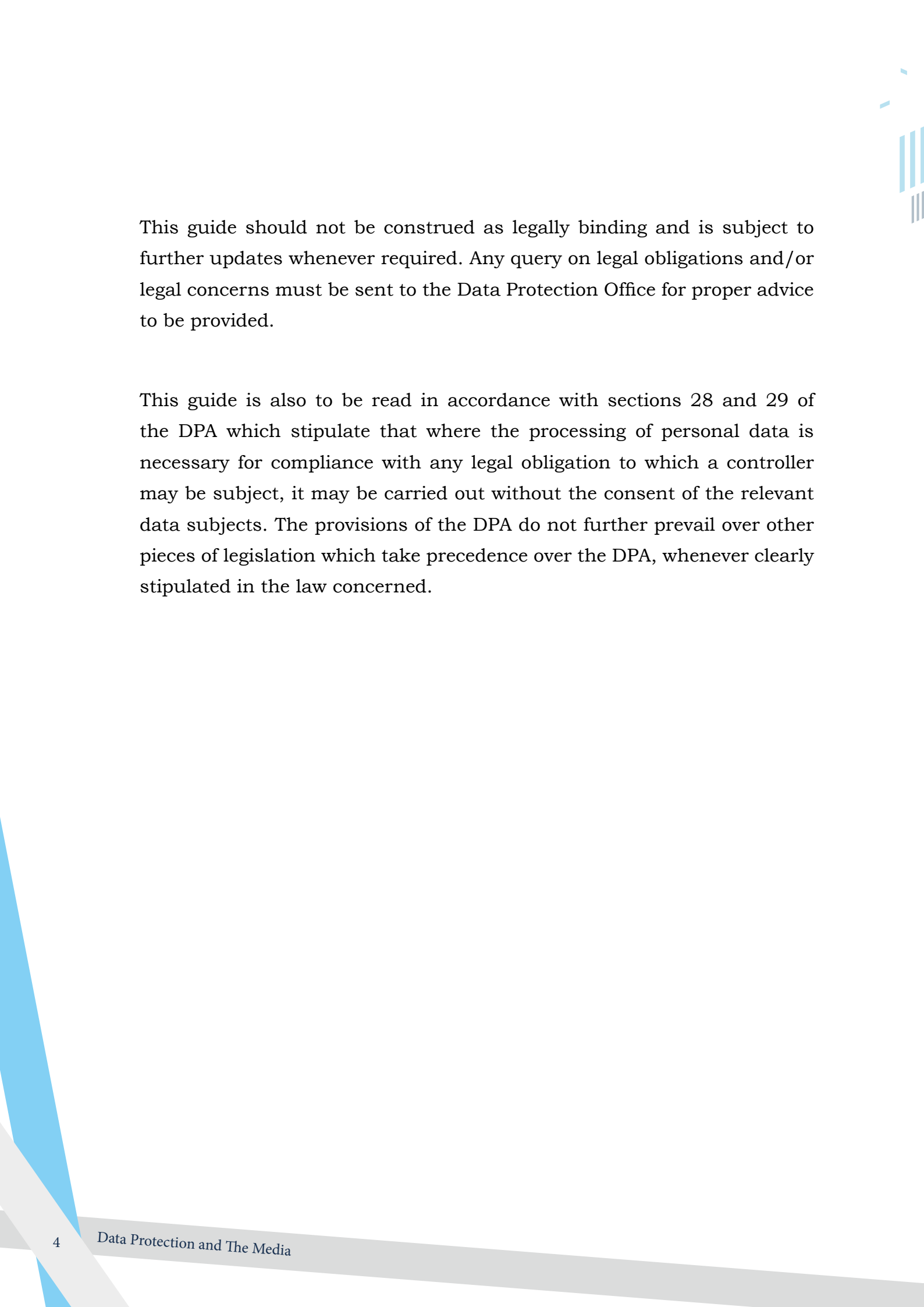
Media professionals process large amounts of personal data when preparing daily news and articles. It is crucial that media organisations and professionals understand their roles and responsibilities to ensure that the privacy rights and ethics of individuals are respected.

The purpose of this guide aims at safeguarding the privacy of public figures and private persons. It elaborates on a general recommended approach towards compliance with the Data Protection Act (DPA) 2017 and best practices.

The DPA does not aim at hampering responsible journalism and this guide explains how media organisations can comply with data protection principles while maintaining a free and independent role.

This guide consists of five main sections covering freedom of expression, the duty of media to disseminate information and responsible journalism, private life and publication of private matters, concerns of private life, crime reporting and best practices and behaviours. It also covers the powers of the Data Protection Office and the obligations on media organisations including registration with the Data Protection Office. In addition, the guide describes the requirements that media organisations must observe for processing operations likely to present high risks to individuals and for data transfers outside Mauritius. It also elaborates on the rights of data subjects and exceptions found under the Data Protection Act.





This guide should not be construed as legally binding and is subject to further updates whenever required. Any query on legal obligations and/or legal concerns must be sent to the Data Protection Office for proper advice to be provided.

This guide is also to be read in accordance with sections 28 and 29 of the DPA which stipulate that where the processing of personal data is necessary for compliance with any legal obligation to which a controller may be subject, it may be carried out without the consent of the relevant data subjects. The provisions of the DPA do not further prevail over other pieces of legislation which take precedence over the DPA, whenever clearly stipulated in the law concerned.



## 2. FREEDOM OF EXPRESSION, THE ROLE OF THE MEDIA AND RESPONSIBLE JOURNALISM

### 2.1. Freedom of expression

Freedom of expression is one of the sustaining pillars of a democratic society since the right to freedom of expression is afforded constitutional protection. It secures everyone's right to speak and write openly as well as the right to criticise injustices and illicit activities. In Mauritius, media organisations play a vital role in this respect to impart information on matters of public interest to citizens. Diversity of opinions in the media must be encouraged to reflect open-mindedness.

The right to freedom of expression is guaranteed under section 19 of the Universal Declaration of Human Rights as follows:

*“Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”*

Section 12 of the Constitution of Mauritius also stipulates that:

“(1) Except with his own consent, no person shall be hindered in the enjoyment of his freedom of expression, that is to say, freedom to hold opinions and to receive and impart ideas and information without interference, and freedom from interference with his correspondence.

(2) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision –

- (a) in the interests of defence, public safety, public order, public morality or public health;
- (b) for the purpose of protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence,

maintaining the authority and independence of the courts, or regulating the technical administration or the technical operation of telephony, telegraphy, posts, wireless broadcasting, television, public exhibitions or public entertainments; or

(c) for the imposition of restrictions upon public officers,

except so far as that provision or, as the case may be, the thing done under its authority is shown not to be reasonably justifiable in a democratic society.”

Generally, it is observed that section 12 of the Constitution elaborates both on the right to freedom of expression and also on the limitations to this right.

## **2.2. Media as public watchdogs with rights and responsibilities**

Media professionals are often perceived as “watchmen” or “guardians” having the role of alerting people as soon as a problem is identified. Their role is to supply citizens with information they must have on matters of public interest. Watchdog journalism spans across a wide range of matters and includes amongst others scandals, financial wrongdoings, corruption and other illegal doings.

However, the right to freedom of expression is not absolute or immune from legal restrictions. This freedom entails certain responsibilities. Consequently, media professionals are bound by rights and responsibilities and have the foremost duty to impart information in a manner consistent with their obligations and responsibilities. Journalists must exercise their functions by reporting sincerely matters of public interest. In addition, they must follow a professional code of ethics by disseminating factually correct and trustworthy information.

Journalists must act in good faith by demonstrating accurate and well-balanced reporting, alteration of incorrect information, clear difference between reported information and opinions, prevention of calumny and respect for privacy and fair trial. Proper verification of facts must be made prior to publishing information. However, this may not apply when opinions are reported. Nonetheless, even where a statement represents an opinion, there must exist sufficient factual basis to sustain it. In the case *Bodrožić v. Serbia*, the European Court of Human Rights accepted a journalist's criticism towards a historian by referring to the latter as 'fascist' on the basis that the expression used by the journalist has to be interpreted as his opinion which was not excessive in light of circumstances related to the case.

Before publishing any article, media is responsible for verifying the accuracy of factual statements by performing adequate checks and verifying the nature of public interest at stake. In rare occurrences, it may be acceptable for media professionals to bypass verification. For example, it may be acceptable where a story is required urgently and is strongly justified in the public interest but the short deadline makes it unreasonable for a complete accuracy check or where the reporting is made using official reports from government.

Media professionals enjoy a certain degree of freedom on the way they present articles. They can use a certain extent of exaggeration or provocation provided that they do not distort any facts or mislead people.

Court injunctions also have an influence on the reporting made by journalists. Sometimes, the Court may give injunctions to stop all publications on a given matter. It is thus very important that judicial authorities undertake a proper assessment when giving injunctions because sometimes delays in disseminating information may result in the loss of interest and value of the information itself.

It is recommended for media professionals wherever practical to seek comments from the people they feature in their articles, notwithstanding the fact that the press does not have any formal obligation to do so. The

European Court of Human Rights also decided in the case of *Mosley v. UK* that newspapers are not required to provide a notice of intention to print stories on an individual's private life.

### **2.3. Responsible journalism v. tabloid journalism**

Responsible journalism is essentially journalism that demonstrates reasonable professional standards in reporting. It reflects a judicious level of care to verify potential offensive/defamatory statements and an adequate examination for corroboration. It depicts accurate facts to people and is driven by truth, fair commenting and public interest.

On the other hand, tabloid journalism emphasizes mostly on journalism that creates sensationalism, very often invading the privacy rights of individuals, and causing harassment to people. It may be described as a form of lucrative commodity exposing the private lives of people in the public eye.

Media professionals are bound by the laws of Mauritius. Therefore, the right to freedom of expression is not the ultimate right for the media sector. It has to be balanced with the privacy rights of individuals and any other applicable laws in force. Journalists promoting tabloid journalism are more at risks of infringing privacy laws. For instance, the private lives of well-known persons are unlikely to be a matter of public interest. Photos taken covertly and without consent are likely to violate the Data Protection Act 2017, as was decided by the French Court verdict holding that paparazzi photos of the Duchess of Cambridge on holiday were an invasion of the royal couple's privacy.

As a rule, violating any law is an offence and may only be justified on assessment by a Court of law where the Court will decide whether the interest of informing the people overrides the obligation to abide by criminal law principles. For instance, a journalist who unlawfully buys drugs to show that drugs are easily available on the market may expect to be prosecuted.

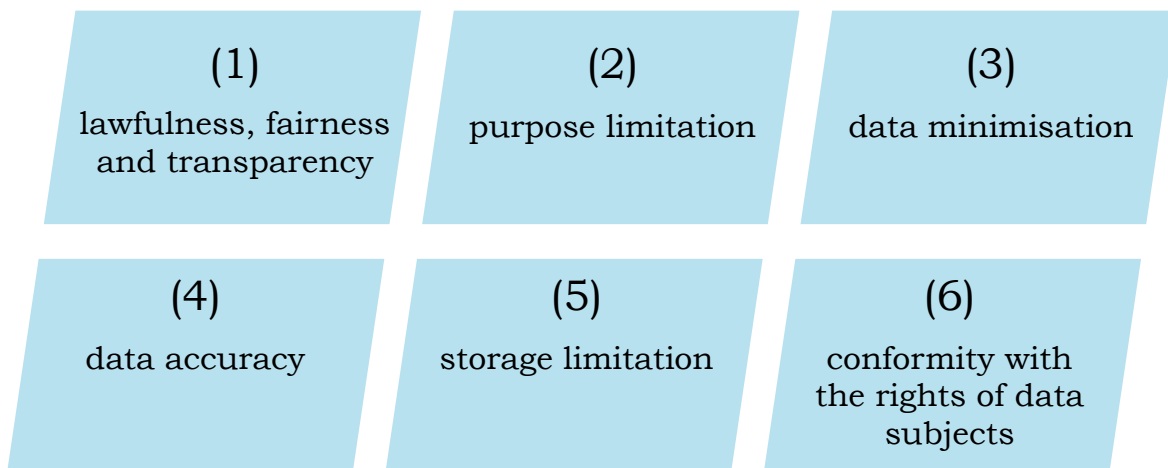


## 3. PRIVATE LIFE AND CONDITIONS FOR PUBLISHING PRIVATE MATTERS

### 3.1. Private life

The Data Protection Act 2017 safeguards the privacy rights of individuals in Mauritius including private and public individuals. This legislation governs the processing of both personal data and special categories of personal data.

Under the DPA 2017, the processing of personal data must comply with the 6 principles relating to processing of personal data namely on



In general, the processing of a purely private matter of an individual such as the latter's sexual life requires the consent of the individual unless it is justified in the public interest. Very often, these publications are for entertainment purposes rather than education.

Media professionals have the responsibility to make a proper assessment of the margin between the private and public spheres on a case-by-case basis to avoid any contravention of the law. As the matter becomes more sensitive, the stronger the justification for processing must be.

### 3.2. Consent

As a general rule, consent is one of the lawful grounds on which personal data may be processed i.e. if there is no consent by an individual then

information about him or her may not be published. An example to illustrate this point is whenever images of individuals are published which may affect them, then those images may be blurred before being published if no consent has been obtained from the data subject when it was legally required.

Based on cases of law, there is a need to make a balance of the private life of a person, the harm caused to that person and the public interest pursued by the publication. Consent is an important element in determining whether a publication of a detail from someone's private life interferes with his/her right to privacy.

The general rule is that there is a need for caution from journalists when the matter is more private if a publication has no prior consent from the data subject.

However, in any publication without consent, the rule is: the more private the matter, the greater the call for caution. For example, a person's romantic relationships are in principle a strictly private matter. Accordingly, details concerning an individual's sex life or intimate relations are only permitted to become public without consent in exceptional circumstances whenever justified by law. This was the case in *Couderc and Hachette Filipacchi Associés v. France*, elaborated below.

### **3.3. Public interest**

It is practically impossible to give a definition of public interest and the editor's codebook explains it as follows:

"The public interest includes, but is not confined to:

- Detecting or exposing crime, or the threat of crime, or serious impropriety.
- Protecting public health or safety.

- Protecting the public from being misled by an action or statement of an individual or organisation.
- Disclosing a person or organisation's failure or likely failure to comply with any obligation to which they are subject.
- Disclosing a miscarriage of justice.
- Raising or contributing to a matter of public debate, including serious cases of impropriety, unethical conduct or incompetence concerning the public.
- Disclosing concealment, or likely concealment, of any of the above."

The following areas are also considered to be of public interest: the misuse of public office, improper use of public money, social behaviour and similar political and socioeconomic topics. There is a non-exhaustive list of public interest scenarios.

Similarly, matters that affect the public to such an extent that it may rightfully take an interest in them, attracting its attention or concerning the public significantly, are considered to be of public interest.

Journalists may publish personal information when it serves a greater value and is used to discuss a matter in the public interest (published personal information should serve some important purpose).

Journalists may republish personal information already made public by the data subject provided that the published information is a matter of legitimate public interest. This is supported by European case law (*Eerikainen and others v. Finland*).

In general, journalists have to apply the public interest test on a case by case basis in order to publish or not personal data related to public interest.



In determining public interest, what should matter to journalists is whether the news report is capable of contributing to a debate of general interest and not whether they will manage to fully achieve that objective.

In *Erla Hlynsdottir v. Iceland (no. 2)*, a journalist reported that the director of a Christian rehabilitation centre and his wife had been involved in sex games with the patients of the centre. Although the wife was not ultimately convicted, reporting about the allegations, which involved private sexual activities, contributed to the public interest.

Matters that bring about considerable controversy, debate or arouse the interest of the public to be informed are generally considered as public interest. However, exposing the private life in media just to create sensationalism cannot be considered to be a matter of public interest. The Max Mosley case is an example where media has been sued for publishing about the private life of the person which has nothing to do with public interest.

### **3.3.1. Public figures**

Public figures are persons who hold public office and/or use public resources. This can include anyone with a role in public life irrespective of whether the field is politics, economy, arts, social, sports, film industry or others. The issue of whether public figures are known to the public is irrelevant for journalists to report on them.

Public figures have to accept that the roles that they play in society automatically limits their private life and media reports on them regularly due to the affinity that readers have for them.

Public figures inevitably and knowingly lay themselves open to close scrutiny of their every word by both journalists and the public at large. Their right to keep their private life protected from the eyes of the public is, therefore, more restricted.

Freedom of expression in the domain of politics would be affected if public figures could censor the press and public debate in the name of personality rights.

The role or function of the concerned person and the nature of the activities subject of the news report have to be taken into consideration by journalists when reporting matters regarding private aspects of life. For example, Princess Caroline von Hannover is considered to be a public figure but does not exercise any official functions, which allows her the right to enjoy a higher degree of privacy than that enjoyed by a person holding a public office.

Politicians are public figures with the lowest expectation of privacy. The exercise of a public function or aspiration to political office necessarily exposes an individual (also after death) to the attention of the public, including in many areas that come within one's private life. The case law *Editions Plon v. France* describes that the disclosure of medical information of the former French President in the book written by the journalist and the former private medical physician is in the domain of public interest.

There are private actions carried out by public figures that cannot be considered as private because of the potential impact it has as perceived by the role played by those public figures in the social or political fields or the interest that is generated in the public being informed. For example, it is a matter of public interest to report on a famous cinema actor (who might be considered as a role model for young people) for the possession and use of illegal drugs.

Journalists should respect the legitimate expectations of public figures to privacy when they engage in purely private activities such as participating in sports, walking, leaving a restaurant or when on holiday or in intimate relationships (marital problems, extramarital affairs) if the reporting does not contribute to a matter of public interest.

### **3.3.2. Private individuals**

In general, private individuals have greater rights to privacy as long as they have not entered the public sphere. However, journalists may report on them if they enter the public domain through their actions. Thus, journalists do not have a complete ban on reporting on them even without their consent.

The case law *Standard Verlags GmbH v. Austria* (no. 3) illustrates the circumstance where a newspaper has reported on a banker with his name published and the ensuing prosecution. The banker was also the son of a politician. The court ruled that while the banker could not be considered as a public figure, the journalist was justified to publish his name because the banker headed the treasury of the bank at the time the losses were incurred.

## **3.4. Framework for balancing the rights to privacy and freedom of expression**

### **3.4.1. Contribution to a debate of general interest**

The decisive factor that a journalist must take into account before disclosing information about someone's private life is whether the article can generate a debate of general interest. This approach is not different from that of public interest. Therefore, a debate that contributes to general interest also leads to the objective of "public interest".

The following examples from court cases explain the point: In *Couderc and Hachette Filipacchi Associés v. France*, a French magazine reported about the child fathered out of wedlock by Prince Albert II of Monaco. Publishing this information served the public interest to be informed about the rules of succession, which might prevent children born out of wedlock from succeeding to the throne. In addition, family members of the monarchy are also part of contemporary history; hence there is an element of public interest in their private lives.

In *White v. Sweden*, two newspapers published a series of articles in which various criminal offences were ascribed to Anthony White by a number of sources, including the murder of the former Swedish Prime Minister, Olof Palme in 1986. The Court considered that the unsolved murder of Olof Palme and the investigation carried out were matters of serious public interest and concern.

In the case of *Selistö v. Finland*, a journalist was convicted and fined for having defamed a surgeon by writing two articles alleging that a patient had died as a result of the surgeon's alcohol consumption during the night preceding the operation. The Court found that recounting the personal experiences of the surviving widower as well as matters of patient safety, concerned an important aspect of health care and as such raised serious issues affecting the public interest.

In *Guseva v. Bulgaria*, a representative of an association working on animal rights protection obtained three final court orders requiring a mayor to provide her with information relating to the treatment of stray animals found on the streets of the town over which he officiated. The treatment of animals was considered to be a matter of general interest and to contribute to public debate.

In the case of *Schweizerische Radio- und Fernsehgesellschaft SRG v. Switzerland* the prison refused to allow a television station to carry out a televised interview inside a prison with a prisoner serving a sentence for murder. The media outlet had intended to broadcast the interview in one of the longest-running programmes on Swiss television. The Court stated that there is no doubt that a report about a convicted murderer who had always protested her innocence attracted public interest and contributed to the discussion about the proper functioning of the justice system.

However, pictures and information of a purely personal nature are not considered to contribute to a debate of general interest. In *Von Hannover v. Germany*, publishing pictures of Princess von Hannover participating in sports without her consent resulted in a violation of her right to privacy.

### ***3.4.2. The role of the person concerned and the subject of the report***

As discussed previously, a private individual unknown to the public may seek protection for his or her right to private life. However, this may not be true for public figures mainly where politicians are involved.

In *Renaud v. France*, the applicant was convicted in criminal proceedings of defaming and publicly insulting a citizen discharging a public mandate, on account of remarks published on the website of an association of which he was president and webmaster. The Court was of the opinion that when a debate relates to an emotive subject, such as the daily life of the local residents and their housing facilities, politicians must show a special tolerance towards criticism.

In *Feldek v. Slovakia*, a research worker in the field of literature published an autobiography where he described, inter alia, his conviction by a Soviet military tribunal on the ground that he had been ordered to spy on the Soviet army. He later became Minister for Culture and Education of the Slovak Republic and the press covered parts of the book. The Court considered that he inevitably and knowingly laid himself open to close scrutiny of his words and deeds by journalists and the public at large, and he must consequently display a greater degree of tolerance.

A different rule applies to civil servants because they do not deliberately expose themselves open to close scrutiny of their every word and deed to the extent to which politicians do. Therefore, media and journalists should treat them differently to how they treat politicians when it comes to the criticism of their actions.

Journalists should pay special attention when reporting on vulnerable groups or those having special needs. For example, children and young people should be given greater protection due to the implicit susceptibility that their age implies in media coverage. When quoting children, extreme care has to be given because of their immaturity and media should have an ethical obligation not to potentially cause harm to a child.

Furthermore, in cases where parents or guardian made negative, sensitive or other inappropriate comments about children under their responsibility, journalists should pay particular attention to the best interests of the child. They should only publish such information when there is a compelling public interest by avoiding to mention the name of the child. This will avoid a lifelong link with negative or embarrassing remarks or opinions.

In such cases, where the name of the child is not cited and images not shown, journalists should also avoid publishing additional information indirectly identifying the child (for example photographs of the parents or the precise location of the family, etc.). When doing research among people who require protection, caution has to be applied, in particular to persons who are mentally or physically impaired or emotionally affected. Journalists should refrain from taking advantage of the vulnerability of these persons to extract information.

### **3.4.3. *Prior conduct of the person concerned***

One of the principles for the processing of personal data as per section 21 of the DPA is purpose limitation. That is, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Thus, personal information obtained for one story cannot be used for another purpose/story unless there is a valid reason to do so. Having worked with or cooperated with the media or journalist in the past (e.g. interviews) may not be used as a valid argument for depriving the person concerned from his right to privacy.

A public figure's voluntary disclosure of information might nevertheless weaken the degree of protection to which that person is entitled. In *Hachette Filipacchi Associés ("Ici Paris") v. France*, a journalist wrote an article on a famous singer (accompanied by photographs) referring to the singer's extravagant financial difficulties and exorbitant tastes. The singer claimed a violation of privacy, but without success, since he had already disclosed information about the lavish way he managed and spent his money in his autobiography, from which the journalist drew information.

### **3.4.4. *Method of obtaining information and its veracity***

Section 23 of the Data Protection Act states that a controller (in this case can be a media organisation or journalist) shall not collect personal data unless it is done for a lawful purpose connected with a function or activity of the controller and the collection of the data is necessary for that purpose.

Thus, the DPA expects you to collect personal information in a fair way that is:

- for a journalistic purpose;
- where practical, informing the person that you are collecting his/her information, who you are, and what you are doing with their information in accordance with section 23 (2) of the DPA;
- only use a data subject's information as he/she would reasonably expect.

Given the nature of the work as a journalist, where it is not possible to inform the person that you are investigating on them, you will need to provide a strong justification, which will support the privacy intrusion.


When collecting special categories of personal data, you should make sure that it is necessary or relevant and for the public interest to justify the privacy intrusion.

Only use secret methods for obtaining information if you are confident that this is justified in the public interest and not prohibited by law. In *Von Hannover v. Germany*, using long lens cameras to secretly take pictures of the princess while she was on holiday was not considered a 'fair way' to obtain information.

#### **3.4.5. Content, form and consequences of publications**

As per the Data Protection Act, accuracy is one of the six principles relating to the processing of personal data. Regarding the content of a news/story, media organisations and journalists should take reasonable steps to check facts correctly to ensure the published data is accurate. They should also take particular care to distinguish between facts, opinion and speculation to avoid any undue harm to the privacy of any individual. In other words, journalists will need





to assess personal data required to report news or story, balance it against the level of intrusion into the life of the data subjects, and the potential harm this may cause.

News can be disseminated in various ways. It can be through printed newspapers, blogs, online newspapers among others. This is also an important element as online news tend to have more impact on the public than printed news. Thus, it is crucial for journalists to ensure content is well prepared and accurate.

Subject to section 42 of the DPA, any controller(whether media organisation or journalist) who, without lawful excuse, discloses personal data in any manner that is incompatible with the purpose for which such data has been collected shall commit an offence. Hence, media organisations and journalists are bound to act in good faith and to make sure the personal information obtained is necessary for publication.



## 4.

# SPECIFIC ISSUES OF PRIVATE LIFE

### 4.1. Family, home, property

Media organisations and journalists should take particular care when publishing content on family members, relatives and friends of public figures. It is to be noted that these people are not public figures and deserve a higher degree of privacy. However, there are cases in which journalists are allowed to report about them. In *Flinkkilä and Others v. Finland*, publishing the name, age, picture, workplace and family relationship details of the partner of a public figure was not considered to be in violation of privacy because she was involved in a domestic incident which had resulted in public disorder charges (both being criminally charged, fined and convicted).

Furthermore, personal information on a suspect's family, his/her occupation, religious background, nationality, race or membership in some organisations should be published only if it is directly relevant for the case and the story.

As per section 30 of the DPA, no person shall process the personal data of a child below the age of 16 years unless the child's parent or guardian gives consent. Hence, when reporting an article on minors, particular care should be taken not to divulge the name and other personal data of the child. Failure to do so will result in a potential breach of the DPA.

Concerning home, a person home address is personal data and should not be made public by the journalists. For example, when reporting a news about a burglary which happened at the house of a data subject, you should not give the exact detailed address of the grieved person.

### 4.2. Physical and moral integrity

The physical and mental health of a data subject is considered as a special category of personal data and is subject to a higher level of protection than the other types of data such as the name, date of birth, or family situation. Journalists should have lawful reasons for processing (publishing) medical

information of a patient or public figures in accordance with section 29 of the Data Protection Act 2017.

In general, it will not be easy for media organisations to justify reporting about intimate life or relationship of a person or even of that of public figures if it is not in connection with a debate regarding general interest. Taking the example of the case of *Standard Verlags GmbH v. Austria (No.2)* where a newspaper published an article commenting on rumours that the spouse of the then Austrian President looked to separate from him and was keeping up close contacts with another politician. This violated the privacy of the persons concerned according to the court. The court also indicated that journalists could report information on the conditions of health of politicians but not on rumours on their marriages.

### **4.3. The right to one's image**

As per the European Court of Human Rights factsheet: “a person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers.” A person image is, therefore, personal data. Every data subject has the right for the protection and usage of his/her own image.

As indicated above, consent is one of the lawful grounds on which personal data processing has to be based, pursuant to section 28 of the DPA. Consequently, journalists will have to secure the consent of the person concerned at the time the picture is taken. However, it is to be noted that section 28 of the DPA provides exceptions where consent may not be required as provided below:

- 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. or 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.

Journalists may invoke section 28 (b)(iv) in the performance of their duties. For example, there will be a public interest in the wide range of media output, from day-to-day stories about local events to celebrity gossip to major public interest investigations. However, this does not automatically mean that publication is always in the public interest. Media organisations and journalists should balance the publication with the fundamental privacy and data protection rights of the person concerned. They would be required to provide justifications in case the publications and investigations are intrusive to the person's personal life.

As pointed in sections above, pictures taken without the consent of the people concerned or covertly without their knowledge will result in a potential breach of the DPA except if they are considered to add to a discussion of public interest, which should be justifiable.

#### ***4.3.1. Specific cases of photographing and filming***

##### **Von Hannover (no. 3) v. Germany (n° 8772/10) 19, September 2013**

Princess Caroline von Hannover filed a complaint when the German courts refused to grant an injunction to prohibit further publication of a photograph of her and her husband which was taken without their knowledge while on a holiday. The photograph was published in an article themed the trend amongst the very wealthy towards letting out their holiday homes.

No violation of the right to respect for private life (Article 8) was found as the Courts had considered all essential criteria and balanced the different interests at stake. The Court accepted that the photograph contributed to a debate of high interest and was therefore not unreasonable.

##### **Schüssel v. Austria, 21 February 2002**

The Deputy Prime Minister of Austria complained in particular about the use of his picture on stickers which was half-overlapped by the face of the right-wing politician Jörg Haider and with the following slogan: “The social security slashers and the education snatchers share a common face”.

The Court declared that the complaint was manifestly ill-founded and the Austrian Supreme Court had correctly weighed the general interest in an open political debate as protected by Article 10 (freedom of expression) of the Convention against the applicant’s interest in protection against the publication of his picture.

##### **Peck v. the United Kingdom, 28 January 2003**

The applicant was suffering from depression and complained about the disclosure of footage to the media from a CCTV camera located

on a street which showed him walking alone with a kitchen knife in his hand. Subsequently, he attempted suicide by cutting his wrists but it was not shown in the CCTV footage. This resulted in having images of himself being published and broadcast widely. Furthermore, he complained of the lack of an effective domestic remedy in that regard.

The Court found that the disclosure of the footage by the municipal council was not done with sufficient safeguards and it constituted a disproportionate and unjustified interference with the applicant's private life, in breach of Article 8 (right to respect for private life) of the Convention. Furthermore, at the relevant time, the applicant did not have an effective remedy for breach of confidence, in violation of Article 13 (right to an effective remedy) read in conjunction with Article 8 of the Convention.

### **Hachette Filipacchi Associés v. France, 14 June 2007**

The weekly magazine Paris Match published an article entitled "La République assassinée" (The Murdered Republic) a few days after the murder of a French prefect. It was a two-page coloured photograph taken moments after the murder which showed the prefect's lifeless body lying on the ground in a pool of blood, facing the camera.

The prefect's widow and children lodged an urgent application with the Courts seeking the seizure of the copies of any magazine in which the photograph appeared and prohibition of their sale on penalty of fines as the photograph of the prefect had been published without the family's consent.

The Court held that there had been no violation of Article 10 (freedom of expression) of the Convention and the French courts had given reasons which were both relevant and sufficient, had been proportionate to the legitimate aim it pursued – to protect of the rights of others, and therefore necessary in a democratic society.

However, the Court observed that the result of the publication of the photograph in a magazine with a very high circulation, had heightened the trauma felt by the victim's close relatives, so they were justified in arguing that there had been an infringement of their right to respect for their private life.

Then examining to what extent the punishment might have a dissuasive effect on the exercise of freedom of the press, the Court noted that the French courts had refused to order the seizure of the offending publications.

### **Khmel v. Russia, 12 December 2013**

The applicant was a member of the Murmansk regional legislature who was taken to a police station on suspicion of drunk driving. He refused to give his name, behaved in an unruly manner and refused to leave the building when asked to do so.

The police chief invited television crews to the station and the applicant was filmed whilst in a disheveled state and acting inappropriately. Some of the footage was broadcast on public television the next day. Administrative and criminal proceedings were later brought against him for his actions on the day he was filmed. The applicant complained in particular about the filming of him at the police station and the broadcasting of the footage, which he claimed to be unlawful.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention, as the release of the video recording to the regional television was not done with the consent of the applicant and it was thus a flagrant breach of the domestic law. The interference with the applicant's right to respect for private life was therefore not "in accordance with the law" within the meaning of Article 8 of the Convention.

### **4.3.2. Correspondence**

In *Leempoel & S.A. ED. Ciné Revue v. Belgium*, a judge was providing evidence in a parliamentary inquiry about a case and was asked to hand over the file she had brought with her in preparation. The file included personal notes about her defence and recommendations from her lawyer as to how to communicate and conduct herself before the commission.

A magazine article was published with lengthy extracts from the preparatory file. The Court found that her privacy was violated because the article contained criticism of the judge's character and included a copy of correspondence that was private and which could not be regarded as contributing in any way to a debate of general interest to society.



## CRIME REPORTING

When reporting about crimes, journalists must pay particular attention as to whether the person concerned is known to the public. The mere fact that a person is subject to criminal investigation, even for a very serious offence, does not justify treating him or her in the same manner as a public figure who is more exposed to publicity.

### 5.1. General principles

The public has a legitimate interest in being informed about crimes, investigation proceedings and trials. While the aim of crime reporting is to inform the public, journalist should nevertheless report in good faith by refraining from publishing groundless and unverified accusations.

In particular, journalists should not present a person as guilty until a sentence has been pronounced by a court. Conviction and suspicion must be clearly demarcated. As a matter of good practice, the media could specify whether a person has pleaded guilty or not by taking into consideration that a confession of guilt should not be presented as a proven guilt.

### 5.2. The right of victims (minors) to protect their identity

In *Krone Verlag GmbH & Co KG and Krone Multimedia GmbH & Co KG v. Austria*, the identity of a minor victim of sexual abuse was revealed in a newspaper by publishing her photograph. Although the issue was a matter of public concern but given that both the offenders and the victim were not public figures, the disclosure of their identity was not necessary to understand the particulars of the case.

As per the Court, the child was not a public figure and she should not enter the public scene through becoming the victim of a criminal offence which attracted considerable public attention.

### **5.3. The right to privacy of a presumed pedophile**

In *Y v. Switzerland*, a journalist was found to violate the right to privacy of a person who was prosecuted for pedophilia and who was eventually released. The article contained considerable detailed information and extracts from the complainant's statements to the police, which was deemed to be in violation of his right to privacy as it did not contribute to a public debate.

### **5.4. Revealing the identity of an investigated police officer**

In *Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft v. Austria*, a news magazine published an article with excerpts of the minutes of preliminary investigations in criminal proceedings against three foreign police officers who were on a deportation flight. The deportee that was being escorted had died under unclear circumstances. The Court ruled that the disclosure of the identity of one officer by the news magazine had negatively affected his private and social life and particular care had to be taken to protect him against a condemnation by the media.

### **5.5. Suspected persons**

Journalists are, in principle, allowed to publish pictures of public figures who are under investigation, for e.g. on the suspicion of large-scale tax evasion. In *Verlagsgruppe News GmbH v. Austria (no.2)*, the newspaper published an article about pending investigations on suspicion of large scale tax evasion against the managing director of a well-known pistol manufacturer. The reporting was not considered to violate the right to privacy of the managing director.

However, journalists must ensure that more care is taken when lesser known persons are in question.

In the case of *Khuzhin and Others v. Russia*, publishing pictures of passports of persons (in a talk show) charged with kidnapping and torturing a few days before their trial resulted in a violation of their right to privacy.

### **5.6. Publishing banal aspects of accused persons**

In *Bedat v. Switzerland*, a journalist was considered to have violated the right to privacy of a person who was accused of three deaths in connection to a car accident.

The Court deemed that publishing records of interviews, statements by the accused's wife and doctor as well as letters sent by the accused to the investigating judge concerning banal aspects of his everyday life in detention did not contribute to a public debate.

Additionally, the Court stated that the journalist had painted a highly negative picture of the accused person. With the use of large close-up photographs of the accused, the journalist sought to create a sensationalist article.

### **5.7. Persons in custody**

In *Toma v. Romania*, some police officers invited journalists to record pictures of the person who was taken in custody for possession of drugs at the police headquarters. The Court found that this person's right to privacy had been violated.

### **5.8. Convicted persons in emotional situations**

In *Egeland and Hanseid v. Norway*, two newspapers had published photographs of an individual who was about to be taken away to serve a long prison term to which she had just been sentenced. The photographs were taken without her consent.

Although the photographs concerned a public event in a public place at a time when her identity was already well known to the public, the Court found that the newspapers' depiction had been particularly intrusive as she was in great distress. She had just been arrested inside a courthouse after having been notified of a verdict convicting her of triple murder and which entails the most severe sentence.

### **5.9. Convicted persons released on parole**

Public authorities, especially law enforcement bodies, often release pictures of wanted, arrested or released-on-parole persons. In principle, journalists are allowed to publish such pictures again. In *Österreichischer Rundfunk v. Austria*, it was deemed acceptable to broadcast the picture of the head of a neo-Nazi organisation, who had been released on parole.

According to the Court, his interest not to have his physical appearance disclosed was not more important than the fact that he was a notorious person who had committed crimes of a political nature.



6.

## **CODES OF CONDUCT AND SELF-REGULATORY TOOLS**

Codes of conduct and self-regulatory bodies or mechanisms comprising publishers, journalists, media users' associations, experts from the academic world and judges are vital for a balanced and ethical practice of journalism.

Generally, journalists are encouraged to comply with these self-regulatory tools.

## DATA PROTECTION PRINCIPLES

### 7.1. Functions of the Data Protection Office

As a regulator with enforcement powers, the Data Protection Office has the mandate to carry out the following functions:

- (a) Ensure compliance with the DPA and any regulations made under it;
- (b) Issue or approve such codes of practice or guidelines for the purposes of the DPA;
- (c) Maintain a register of controllers and processors;
- (d) Exercise control on all data processing operations, either of its own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with this Act;
- (e) Promote self-regulation among controllers and processors;
- (f) Investigate any complaint or information which gives rise to a suspicion that an offence may have been, is being or is about to be, committed under the DPA;
- (g) Take such measures as may be necessary to bring the provisions of this Act to the knowledge of the general public;
- (h) Undertake research into, and monitor developments in, data processing, and ensure that there is no significant risk or adverse effect of any developments on the privacy of individuals;
- (i) Examine any proposal for automated decision making or data linkage that may involve an interference with, or may otherwise have an adverse effect, on the privacy of individuals and ensure that any adverse effect of the proposal on the privacy of individuals is minimised;
- (j) To cooperate with supervisory authorities of other countries, to the extent necessary for the performance of his duties under this Act, in particular by exchanging relevant information in accordance with any other enactment;

## **7.2. Powers of the Data Protection Office**

The Data Protection Act provides a wide range of powers to the Data Protection Commissioner in carrying out the functions and enforcing the provisions of the Act. The powers are stipulated under sections 7, 8, 9, 10, 11, 13, 31 and 46 of the Data Protection Act and are as follows:

- 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
- Compliance audit

### **7.2.1. Power to require information**

The Data Protection Commissioner may, by written notice served on a person, request from that person such information as is necessary or expedient for the discharge of the functions prescribed under the DPA subject to section 26 of the Bank of Mauritius Act, section 64 of the Banking Act, section 83 of the Financial Services Act, section 30 of the Financial Intelligence and Anti-Money Laundering Act and section 81 of the Prevention of Corruption Act.

Where the information requested by the Commissioner is stored in a computer, disc or cassette, or on microfilm, or preserved by any mechanical or electronic device, the person named in the notice must produce or give access to the information in a form in which it can be taken away and in which it is visible and legible.

### **7.2.2. Preservation order**

The Data Protection Commissioner may apply to a Judge in Chambers for a preservation order for the expeditious preservation of data, including traffic data, where he/she has reasonable ground to believe that the data are vulnerable to loss or modification.

### **7.2.3. Enforcement notice**

Where the Data Protection Commissioner is of the opinion that a controller or a processor has contravened, is contravening or is about to contravene the Data Protection Act, the Commissioner may serve an enforcement notice on him requiring him to take such steps within such period as may be specified in the notice.

### **7.2.4. Power to seek assistance**

For the purpose of gathering information or for the proper conduct of any investigation under the Act, the Data Protection Commissioner may seek the assistance of such person or authority as he/she thinks fit and that person or authority may do such things as are reasonably necessary to assist the Commissioner in the discharge of his/her functions.

### **7.2.5. Power of entry and search**

An authorised officer may enter and search any premises for the purpose of discharging any function or exercising any power under the Data Protection Act upon the production of a warrant.

Subject to section 26 of the Bank of Mauritius Act, section 64 of the Banking Act, section 83 of the Financial Services Act, section 30 of the Financial Intelligence and Anti-Money Laundering Act and section 81 of the Prevention of Corruption Act, an authorised officer may, on entering any premises:



- a) request the owner or occupier to produce any document, record or data;
- b) examine any such document, record or data and take copies or extracts from them;
- c) request the owner of the premises entered into, any person employed by him, or any other person on the premises, to give to the authorised officer all reasonable assistance and to answer all reasonable questions, orally or in writing.

Furthermore, where any information requested by the authorised officer is stored in a computer, disc or cassette, or on microfilm, or preserved by any mechanical or electronic device, the person to whom the request is made must produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

#### **7.2.6. Delegation of power by Data Protection Commissioner**

The Data Protection Commissioner may delegate any investigating or enforcement power conferred on him/her by the Data Protection Act to an officer of the office or to a police officer designated for that purpose by the Commissioner of Police.

#### **7.2.7. Prior security check**

Where the Data Protection Commissioner is of the opinion that the processing or transfer of data by a controller or processor may entail a specific risk to the privacy rights of data subjects, he/she may inspect and assess the security measures taken under section 31 prior to the beginning of the processing or transfer.

The Commissioner may, at any reasonable time during working hours, carry out further inspection and assessment of the security measures imposed on a controller or processor under section 31.

### **7.2.8. Compliance audit**

The Commissioner may carry out periodical audits of the systems of controllers or processors to ensure compliance with the Data Protection Act.

## **7.3. Registration**

According to the Data Protection Act 2017, all controllers who process personal data have to be registered with the Data Protection Office. They also have the responsibility of renewing their registration appropriately according to the provisions made in the Act. Therefore, the press company has to ensure that they comply with their registration and renewal requirements. A guide is available on our website to assist controllers at the following URL:

<http://dataprotection.govmu.org/English/Pages/default.aspx> .

## **7.4. Principles relating to processing of personal data**

Controllers and processors have a legal obligation under section 21 of the Act to ensure that the following principles are being observed in their processing of personal data:

- **Transparent & lawful processing:** Personal data must be processed lawfully, fairly and in a transparent manner in relation to any data subject.
- **Purpose Limitation:** Personal data must be collected for explicit, specified and legitimate purposes and not further processed in a way incompatible with those purposes. For e.g Doctor disclosing a list of patients to his wife who owns a travel agency.
- **Data minimisation:** Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **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.

- **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.
- **Data Subjects' rights:** Personal data must be processed in accordance with the rights of data subjects.

### **7.5. Duties of controller**

Every controller (media organisations) should adopt policies and implement appropriate technical and organisational measures to demonstrate that processing of personal data is performed in accordance with the DPA.

The measures mentioned above must include the following:

- Implementing appropriate data security and organisational measures
- Keeping a record of all processing operations as per the template provided on our website
- Performing data protection impact assessments whenever required on high-risk operations as per our guideline
- Complying with requirements of prior authorization and consultation as per section 35 of the DPA
- Designating an officer responsible for data protection (Data Protection Officer).

### **7.6. Collection of personal data**

All controllers must ensure that collection of personal data

- is done for a lawful purpose connected with a function or activity of the controller; and
- is necessary for that purpose.

Controllers must provide a list of information as per section 23(2) while collecting personal data.

However, controllers are exempted to comply with section 23(2) where :-

- (i) the data subjects have already been informed of the list of information required under section 23(1) and (2); or
- (ii) it is impossible or would involve a disproportionate effort and the data are not collected from the data subject or
- (iii) the recording or disclosure of the data is laid down by law and the data are not collected from the data subject.

You may provide a Data Protection Information notification to comply with your obligation to collect personal data. A template is available on our website.

## **7.7. Conditions for consent**

The Data Protection Act 2017 defines consent as “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.”

### **7.7.1. Elements of a valid consent:**

- ‘freely given’ – a data subject must have the choice to accept or refuse to the processing of his /her personal data;
- ‘specific’ – consent of the data subject must be given in relation to “one or more specific” purposes and that a data subject has a choice in relation to each of them. The requirement that consent must be ‘specific’ aims to ensure a degree of user control and transparency for the data subject.
- ‘informed’ – Providing information to data subjects prior to obtaining their consent is essential in order to enable them to

make an accurate judgment, understand what they are agreeing to, and for example exercise their right to withdraw their consent.

- ‘unambiguous indication’ - by statement or a clear affirmative action to avoid implied form of actions by the data subject such as pre-ticked opt-in boxes.

**Note:** *Even if consent meets the four elements described above, it is not a license for unfair and unlawful processing to take place. If the purpose of the data processing is excessive and/or disproportionate, even if the user has consented, the controller will not have a valid legal ground and would be in violation of the DPA.*

### **7.7.2. Section 24 of the DPA**

- The DPA introduces requirements for controllers to make additional arrangements to ensure they obtain, maintain and are able to demonstrate valid consent. Section 24 of the DPA sets out these additional conditions for valid consent, with specific provisions on keeping records of consent and the right to easily withdraw consent.
- Section 24 (2) prescribes that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time. Generally, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent - and in accordance with the DPA - remain lawful, however, the controller must stop the processing actions concerned. If there is no other lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted by the controller.

**Note:** *If the lawful ground for processing is consent, then data subjects can withdraw his consent. It would not be relevant to withdraw consent when other lawful grounds of processing are relied on for processing.*

- Subject to section 24(3), in determining whether consent was freely given, account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

**Note:** *When consent is not necessary for the provision of a service, then you should not require consent. It is thus the responsibility of controllers to determine same. Please also refer to point 2 which is on the exemptions of section 28(1)(b) of the DPA.*

*You need to justify the reason for not providing (terminating) the service to the client when the latter withdraws its consent.*

- There is no specific time limit mentioned in the DPA for how long consent will last. How long consent will last will depend on the context, the scope of the original consent and the expectations of the data subject. Note if the processing operations change or evolve considerably, then the original consent is no longer valid. If this is the case, then new consent needs to be obtained.

Point 3.2 above explains how consent is considered as a lawful ground for processing personal data and how it applies in this sector. Media organisations should thus be very careful when processing personal data and ensure where consent has not been provided that the publication of a story is a matter of public interest.

### **7.8. Notification of personal data breach and Communication to the data subject**

The definition of a personal data breach is provided in the section 'Terms'. An example of a personal breach is: An intruder steals a device containing personal information that has never been published and misuses the information for his personal gain.

Section 21 of the DPA stipulates that in 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. Media organisations and journalists will thus have to comply with this section in the event of a personal data breach.

Section 26 (1) of the DPA states that subject to subsection 26 (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.

As per section 26 (3) of the DPA, the communication of a personal data breach to the data subject shall not be required where –

- (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the breach, in particular, those that render the data unintelligible to any person who is not authorised to access it, such as encryption;
- (b) the controller has taken subsequent measures to ensure that the high risk to the rights and freedoms of the data subject referred to in subsection (1) is no longer likely to materialise; or
- (c) it would involve disproportionate effort and the controller has made a public communication or similar measure whereby data subject is informed in an equally effective manner.

People may not be possibly aware that journalists are conducting investigations upon them. As stated above, journalists should have strong justifications for conducting covert investigations. In case of a personal data breach, media organisations should determine whether same should be communicated to the data subject concerned based on the provisions of section 26 of the DPA. Should the media organisations have any doubt, they can consult the Data Protection Office.

### **7.9. Duty to destroy personal data**

The Data Protection Act requires controllers to destroy personal data where the purpose for keeping personal data has lapsed and to notify any processor holding the data (section 27).

Taking into consideration other applicable laws, media organisations and journalists should destroy personal data as soon as the purpose has lapsed. For instance, for the purpose of a story, a journalist collected personal information of a citizen, however, the story was never and will never be published. Since the purpose has lapsed, the journalist should destroy the data.

### **7.10. Lawful processing**

We have provided explanations on consent in part 3.2 above as well as details on lawful processing in section 4.3.

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. Accordingly, media organisations should ensure that their processing is lawful.

### **7.11. Special categories of personal data**

We stated in section 3.1 which is on private life that the processing of a purely private matter of an individual such as an individual's sexual life requires the consent of the individual unless it is justified in the public interest.

Special categories of personal data is not only about sexual life but also contains other types of data as described in terms above. Consequently, section 29 of the DPA will apply. As per section 29 (1) of the DPA, 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 29(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.

Media organisations and journalists should be very careful and should handle special categories of personal data wisely in order not to contravene section 29. Before collecting or publishing these types of personal data, they must consider whether it is required (i.e. can the story be reported and understood without divulging the data) or whether it is of public interest.

### **7.12. Personal data of child**

According to section 30 of the DPA, no person shall process personal data of a child below the age of 16 years unless the child's parent or guardian

provide his/her consent. Secondly, 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.

Hence, when reporting an article on children, where possible, media organisations and journalists should seek the consent of the parent or guardian and if this is not possible particular care should be taken not to divulge the name and other personal data of the child. Section 5.2 above provides an example of a case regarding a minor whose details have been published and the court concluded that the disclosure of the identity of the child was not necessary to understand particulars of the case.

### **7.13. Security of processing**

Pursuant to section 31 of the DPA, appropriate technical and organisational measures should be implemented for the protection of personal data whether it is stored in manual or automated data filing systems against unauthorised access, alteration, disclosure, accidental loss and destruction. The media are not exempt from these security obligations. Media organisations should take reasonable steps to store personal data securely such that it is not stolen, lost or used deliberately or accidentally.

Media organisations should consider their:

#### **✦ Technical (electronic) security.**

This includes log-on controls, firewalls, encryption, remote wiping facilities, suitable back-ups, and proper disposal of old equipment. Consider both office computer systems and any mobile devices used out of the office (eg smartphones, laptops or tablets). If employees are allowed to use their own mobile devices, refer to your Bring Your Own Devices (BYOD) guidance.

✦ **Physical security.**

This includes locks, alarms, supervision of visitors, disposal of paper waste, and how to prevent notebooks and mobile devices being lost or stolen when staff are out of the office. This may be a particular issue for journalists who spend a lot of time out of the office gathering information or filing reports on location.

✦ **Management and organisational measures.**

For example, ensuring that a person with the necessary authority and resources has a day to day responsibility for ensuring information security, and putting in place robust policies and procedures, including a breach management plan.

✦ **Staff training and supervision.**

Organisations should vet new staff to a level appropriate to their position to confirm their identity, reliability and provide training (including regular refresher training) on key security risks, procedures and responsibilities.

Section 31 also states at subsection 4 that where a controller is using the services of a processor –

- (a) he or it shall choose a processor providing sufficient guarantees in respect of security and organisational measures for the purpose of complying with subsection (1); and
- (b) the controller and the processor shall enter into a written contract which shall 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 subsection (1).

For instance, if a journalist or a media organisation is using the service of another organisation to publish its article on newspapers or TV or through any other medium, section 31 (4) will apply.

#### **7.14. Record of processing operations**

Since the rule is the same for all controllers, media organisations and journalists will have to maintain a record of all processing operations under their responsibility according to section 33 of the DPA. How you will record the processing operations will depend on you, however, the Data Protection Office has designed a template for this purpose which is available on our official website at the following URL: <http://dataprotection.govmu.org/English//DOCUMENTS/TEMPLATE%20FOR%20RECORD%20OF%20PROCESSING%20OPERATIONS.XLS>.

#### **7.15. Data Protection Impact Assessment (DPIA)**

As per section 34, 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 must, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

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.

A DPIA is 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;
- if you are organising a corporate event and you need to know what kind of food the invitees are allergic to, you do not have to carry out a DPIA.
- when the nature, scope, context and purposes of the processing

are very similar to the processing for which a DPIA has 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.

The Data Protection Act 2017 sets out the minimum features of a DPIA:

- a description of the envisaged processing operations and the purposes of the processing;
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged must:
  - (i) address the risks and the safeguards, security measures, mechanisms to ensure the 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:



A form and a list of criteria to evaluate high risk processing are available on the website of this office.

### **7.16. Prior Authorisation and Consultation**

Subject to section 35, every controller or processor must 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.

Authorisation must 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.

### **7.17. Transfer of personal data**

Personal data may only be transferred by controllers and processors outside of Mauritius in compliance with the conditions for transfer as set out in 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 –
  - 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;
  - for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;
  - for reasons of public interest as provided by law;
  - for the establishment, exercise or defence of a legal claim; or
  - 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
  - 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.

### **7.18. The rights of individuals**

Media organisations are considered as “traditional” controllers and must fully comply with data protection requirements to ensure the privacy of individuals.

Under Article 9 of the convention on the protection of individuals with regard to automatic processing of personal data (Convention 108), derogations from basic data protection principles may be allowed, for instance, to ensure the freedom of expression, only when such derogations are provided for by law and constitute necessary measures in a democratic society in the interests of protecting the data subject or the rights and freedoms of others.

Furthermore, as per section 44 of the Data Protection Act (DPA), exceptions may be provided where they constitute a necessary and proportionate measure in a democratic society for:

- a. subject to section 44(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.

Journalists will then need to assess, on a case by case basis, if they are allowed to derogate from the basic data protection principles in specific circumstances.

#### **7.18.1. Right of access**

Individuals have the right to obtain confirmation of whether personal data relating to them are kept as well as a copy of such data free of charge following a written request.

The controller should consider whether information (or some of it) can be provided without undermining its journalistic activities. The request may be refused if the disclosure of the information would impair the journalistic activities (revelation of the sources, of an undergoing investigation, etc.), would infringe the rights of third parties or would affect in a disproportionate manner freedom of expression. In case of refusal to comply with a request, the media organisations should record the reasons for this decision and communicate them to the person concerned.

### **7.18.2. *Right of rectification, erasure or restriction***

Similarly, an individual has the right to request for correction of personal data which he/she believes is inaccurate or incomplete. Or, he/she may also request that his/her personal data are erased if the continued processing of those data is not justified, for example where the data is no longer needed in relation to the purpose for which it was originally collected, the individual withdraws consent, he/she objects to processing and there is no overriding legitimate interest for continuing the processing or data is processed unlawfully.

In addition, an individual may request that the processing of his/her personal data is restricted for example, where he/she contests the accuracy of the data (processing is restricted until the accuracy is verified), objects to its processing (and consideration is being given to whether legitimate grounds override those of the individual), processing is unlawful or data is no longer needed but he/she requires it for a legal claim.

### **7.18.3. *Right to object***

Likewise, an individual has the right to object in writing at any time the processing of personal data relating to him/her free of charge, unless the controller demonstrates compelling legitimate grounds for the processing which override the data subject's interests, rights and freedoms or for the establishment, exercise or defence of a legal claim.

## **7.19. Processing of non-editorial content**

Media organisations and journalists should keep in mind that the data protection principles are fully applicable concerning non-editorial content as well for instance when they process personal data for commercial or administrative purposes.

Therefore, they should also apply data protection principles when they process personal data about their subscribers (for instance for advertising purposes) or about their employees.

Personal data collected for non-editorial purposes shall be only processed if there is a lawful basis for the processing. The existence of a lawful basis for data processing is a precondition for the legitimacy of the processing itself. Along with the existence of such legal ground for data processing, media organisations must take into account the following data processing principles:

Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to any data subject;
- collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay;
- 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; and
- processed in accordance with the rights of data subjects.

All data protection principles shall be considered simultaneously.

## **7.20. Best practices to ensure and demonstrate compliance**

In line with good practice, the media should take all necessary measures to ensure compliance with the data protection requirements and to demonstrate it.

For example, the following accountability tools are useful:

- appointment of a data protection officer;
- establishment of a register of data protection processing activities;
- elaboration of a privacy policy;
- internal procedures to consider the data protection implications at key stages of journalistic activity and to adopt swift decisions in cases of ethical difficulties;
- internal procedures to handle complaints of individuals, to alert the management of the organisation, to contact the data protection office, to deal with cases of security breaches, etc.;
- elaboration of a data protection impact assessment in case of high risks for the individuals;
- regular audits to verify and ensure compliance;
- review the contracts and relations with processors and third parties;
- basic data protection and privacy training for journalists and for the staff members;
- awareness raising activities (clear information for the individuals, dedicated data protection and privacy page on the website or on the intranet; etc.).

Relevant “accountability tools” may also be adapted to the size and resources of the media organisations.

## REFERENCES

- [1] Data Protection Act 2017
- [2] The consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data. 2017. *Guidelines on Safeguarding Privacy in the Media*.
- [3] Information Commissioners' Office. 2004. *Data protection and journalism: a guide for the media*. [ONLINE] Available at: <https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf>. [Accessed 13 November 2018].
- [4] EthicNet. *Journalists Ethics Code*. [ONLINE] Available at: [http://ethicnet.uta.fi/belarus/journalists\\_ethics\\_code](http://ethicnet.uta.fi/belarus/journalists_ethics_code). [Accessed 13 November 2018].
- [5] European Court of Human Rights. 2017. *Right to the protection of one's image*. [ONLINE] Available at: [https://www.echr.coe.int/Documents/FS\\_Own\\_image\\_ENG.pdf](https://www.echr.coe.int/Documents/FS_Own_image_ENG.pdf). [Accessed 14 November 2018].
- [6] European Court of Human Rights. 2009. *Case Of Bodrožić And Vujin V. Serbia*. [ONLINE] Available at: <http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-93157&filename=001-93157.pdf&TID=thkbhnilzk>. [Accessed 26 November 2018].
- [7] European Court of Human Rights. 2011. *Case Of Mosley V. The United Kingdom*. [ONLINE] Available at: [http://www.menschenrechte.ac.at/orig/11\\_3/Mosley.pdf](http://www.menschenrechte.ac.at/orig/11_3/Mosley.pdf). [Accessed 26 November 2018].
- [8] Government Information Service/Geoffrey Robertson QC. 2013. *MEDIA LAW AND ETHICS IN MAURITIUS*. [ONLINE] Available at: <http://gis.govmu.org/English/Documents/Media%20Law%20%20Preliminary%20Report.pdf>. [Accessed 26 November 2018].

- [9] The Guardian. 2017. *Court awards Duchess of Cambridge damages over topless photos*. [ONLINE] Available at: <https://www.theguardian.com/uk-news/2017/sep/05/topless-photos-of-duchess-of-cambridge-were-invasion-of-privacy>. [Accessed 26 November 2018].
- [10] Wikipedia. 2018. *Watchdog journalism*. [ONLINE] Available at: [https://en.wikipedia.org/wiki/Watchdog\\_journalism](https://en.wikipedia.org/wiki/Watchdog_journalism). [Accessed 26 November 2018].
- [11] The Editors' Codebook. *The public interest*. [ONLINE] Available at: <http://www.editorscode.org.uk/downloads/codebook/codebook-the-public-interest.pdf>. [Accessed 7 January 2019].

