THE DIOCESE OF GOZO

GENERAL DECREE ON THE PROTECTION OF DATA

Preamble

1.- Christianity has contributed to the European culture the conviction of the inviolable dignity of the human person, rooted in the fact of the Creation of the human being "in the image and likeness of God". Dignity is, then, an attribute of the rational and free human nature, and its recognition requires adequate protection of personal data.

2.- The Catholic Church, recognizing "the right of each person to protect their own privacy", in accordance with canon 220 of the Code of Canon Law of 1983 (CIC) and canon 23 of the Code of Canon Law of the Eastern Churches of 1990 (CCEO), and upholding that it is a natural right that must respect by all, has been applying a series of principles in relation to the processing of personal data, taking into account, in addition to those cited, and other provisions of private law, the following:

- Canon 535 §§ 1-2 CIC, which requires that the parish books be kept in accordance with the canonical norms.
- Canons 486, 487, 488, 489 and 535 §§ 4-5 CIC, referring to the archives of the diocesan Curia and the parish archives.
- Canons 1339§ 3; 1717, 1719 concerning disciplinary and penal processes.
- Procedural Law, Book VII CIC.

3.- This General Decree does not affect the regulation of ministerial secrecy, nor any other right or obligation of secrecy regulated in Canon Law or the laws of Malta,

4.- Further to the above, and in accordance with the provisions of Article 91 of Regulation (EU) 2016/679, of the European Parliament and of the Council, of April 27, 2016, on the protections of natural persons with regard to the processing of personal data and on the free movement of such data, it was felt necessary that a specific canonical regulation on the protection of personal data be drawn up on the lines of the same substrantial law cited above. This respects, on the one hand, the organizational autonomy of the Church as recognized both in the International Treaties, as well as, in the Maltese Constitution and other local legislation, as a necessary presupposition for the exercise of the right of religious freedom both on an individual and institutional level, indispensable for the existence of pluralism in a democratic society and would allow the continuation of application of the same internal rules relating to the protection of data of natural persons, and, on the other hand, guarantee the aforementioned fundamental right of religious freedom, both to the Catholic faithful, and to those who relate, in some way, with the Church, without prejudice to the application of current civil legislation in this matter.

5.- The adoption and entry into force of this General Decree, which constitutes the particular law of the Catholic Church in the Diocese of Gozo, and which establishes a

substantial level of protection equivalent to the civil order, complementing the European and state regulations on the protection of natural persons with regard to the processing of personal data and their free movement, is intended, in turn, to preserve the required autonomy of the Church. So however that the provisions of this General Decree shall prevail over any norm, custom or practice, as is currently in force within the Diocese, in so far as they regulate data protection matters.

6.- Considering that the exceptions provided for in the EU Regulation with regard to some rights that need to be protected are insufficiently addressed in the same legal framework, the same Regulation allows that the Church, from its own canonical tradition, guarantee and complement an adequate level of protection foreseen in the civil legislation. In this sense, the adoption of a General Decree allows the introduction of clauses that protect the specific interests of the Catholic Church, as a religious denomination, and guarantee its peculiarities.

7.- The content of this General Decree, which has been drafted taking into account the guidelines of the Episcopal Commission of the European Communities, reproduces, where it is considered appropriate, the most significant Articles of the EU Regulation, to facilitate its later application, so that later no need shall arise for excessive references to the European text.

In accordance with the above, and pursuant to cann. 29, 391, and 455 § 4:

DECREES

Chapter 1

General Provisions

Article 1. Object

The object of this General Decree is the protection of the personal rights of natural persons with regard to the processing of personal data; as well as the guarantee that the acquisition, storage and use of data relating to the faithful, by the canonical entities, ecclesiastical associations, is carried out in full respect of the right of the person to the one's good name and confidentiality as recognized by canon 220 of the Code of Canon Law.

Article 2. Scope of material application

§ 1. This General Decree applies to the total or partial automated processing of personal data, and to such other processing other than by automated means where such personal data forms part of a filing system or is intended to form part of a filing system.

Provided that this General Decree shall not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

§ 2. This General Decree does not affect the regulation of ministerial secrecy, nor any other right or obligation of secrecy regulated in Canon Law or the Laws of Malta.

Article 3. Scope of organizational application

§1. This General Decree shall apply to all entities of the Diocese of Gozo, and, in a specific way, to the extent that the processing of personal data has within the activities of the aforementioned entities in the fulfillment of their purposes, regardless of where the processing is carried out, or if it is carried out by an ecclesiastical authority or is carried out in its name.

§ 2. The canonical entities, even those of Pontifical right, as well as entities formed under civil law that are related to the the Diocese of Gozo, may avail themselves of the provisions of this General Decree, after informing the Bishop, and unless the Bishop objects.

Article 4. Definitions

§ 1. "Personal Data" means any information about an identified or identifiable natural person ("data subject"); any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a name, an identification number, location data, an online identifier or one or several elements of the identity: physical, physiological, genetic, psychic, economic, cultural or social of that natural person;

§ 2. "Processing": means any operation or set of operations performed on personal data or on sets of personal, whether or not by automated means, such as collection, registration, organization, structuring, retention, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of access, check or interconnection, restriction, suppression or destruction;

§ 3. "Restriction of the processing": means the marking of stored personal data for the purpose of limiting its processing in the future;

§ 4. "Profiling": means any form of automated processing of personal data consisting of using personal data to evaluate certain personal aspects of a natural person, in particular to analyze or predict aspects related to the professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements of said person;

§ 5. "Pseudonymisation": means the processing of personal data in such a way that they can no longer be attributed to an individual without using additional information, provided that such additional information is kept separately and is subject to technical and organizational measures designed to ensure that personal data is not attributed to an identified natural person or identifiable;

§ 6. "identity unlinking": means the processing of personal data so that details of personal or material conditions can no longer be attributed to an identified or identifiable natural person or are only possible by investing disproportionate time, costs and work;

§ 7. “Filing system”: means any structured set of personal data, accessible according to certain criteria that allow searches by persons or personal data and not merely chronological, whether centralized, decentralized or distributed functionally or geographically,

§ 8. “Data controller”: the natural or legal person, authority, agency or other body that, alone or jointly with others, determines the purposes and means of processing,

§ 9. “Processor”: the individual or legal, authority, agency or other body that processes personal data on behalf of the controller;

§ 10. “Recipient”: the natural or legal person, authority, agency or other body to which personal data is communicated, whether or not it is a third party;

§ 11. “Third party”: the natural or legal person, authority, agency or organization other than the data subject, the processor and the persons authorized to process personal data under the direct authority of the cotroller or the processor;

§ 12. "Consent of the data subject": any free, specific, informed and unequivocal expression, by which the data subject, either through a statement or clear affirmative action (be it verbal, writtebn or electronic), accepts the processing of personal data that concern him/her.

§ 13. “Personal data breach”: means any breach of security resulting from the destruction, loss or accidental or unlawful alteration of personal data transmitted, conserved or otherwise processed, or unauthorized communication or access to said data

§ 14. “Special categories of personal data”: personal data revealing ratial or ethnic origin, political opinions, religious or philosophical beliefs, or trade unión membership, and the processing of generic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

§ 15. “Genetic data”: personal data relating to inherited or acquired genetic characteristics of a natural person that provide unique information about the physiology or the health of that person, obtained in particular from the analysis of a biological sample of such person

§ 16. “Biometric data”: personal data resulting from a specific technical processing, relating to the physical, physiological or behavioral characteristics of a natural person which allow or confirm the unique identification of that natural person, such as facial images or fingerprinting data.

§ 17. “Data concerning health”: personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information about your health status;

§ 18. “Authorities and ‘Church’”: those referred to in the current Code of Canon Law,

§ 19. “Entities of the Catholic Church”: those referred to in Article 3 of this General Decree,

§ 20. “Third country”: means any country or territory outside of the European Economic Area,

§ 21. “Company” means a legal entity composed of an association or society of persons engaged in an economic activity, regardless of its legal form, having a legal personality distinct from that of its members.

§ 22. “Business group”: group constituted by a company that exercises control over its controlled companies;

§ 23. “Resilience”: ability to recover the data protection system after a disturbance of any kind;

§ 24. “Supervisory authority”: the independent authority in charge of data protection control;

§ 25. “Delegate for Diocesan Data Protection”: Person designated by the Bishop in virtue of what is established in Article 33;

§ 26. In addition to workers who actually occupy a job or are hired by an ecclesiastical entity, the following shall be considered as “Employed persons” for the purposes of this General Decree the following:

1. Clergy and candidates for the priesthood,
2. Members of religious orders,
3. Persons who perform work placements or similar activities in an ecclesiastical entity,
4. Persons who carry out volunteer activities through or in an ecclesiastical entity,

§ 27. The duty of confidentiality shall not be waived upon termination of employment.

Chapter II Principles

Article 5. Data secrecy

It is forbidden for any person to process personal data without the authorization of the data controller. The persons authorized by data controller to process data and any person involved in the same way are obliged to maintain the confidentiality of the data and to comply with the regulations on data protection and applicable codes of conduct. These obligations subsist after termination of employment.

Article 6. Lawfulness of the processing of personal data

§ 1. The processing of personal data shall only be lawful if at least one of the following conditions is met:

1. this General Decree or any other ecclesiastical or state norm allows or orders it;
2. the data subject gave his consent for the processing of his personal data for one or several specific purposes;

3. the processing is necessary for the execution of a contract in which the data subject is a party or for the application at the latter's request of pre-contractual measures;
4. the processing is necessary for the fulfillment of a legal obligation to which the controller is subject;
5. the processing is necessary to protect the vital interests of the data subject or another natural person;
6. the processing is necessary for the realization of the proper functions of the Catholic Church or of the powers entrusted to the ecclesiastical authorities;
7. the processing is necessary for the satisfaction of legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child or minor. The provisions of n. 7 of § 1 of this Article shall not apply to the processing carried out by the ecclesiastical authorities in the exercise of their functions.

§ 2. The processing for a purpose other than that which personal data was collected shall be lawful only if:

1. this General Decree or any other ecclesiastical or state norm allows or orders it;
2. the data subject has given his consent,
3. it obviously reflects the interest of the data subject and there is no reason to believe that he would deny consent;
4. the data given by the data subject must be verified because there are specific indications by which it can be assumed that they are incorrect,
5. the data are publicly accessible or the controller might publish them, unless the legitimate interest of the data subject to avoid the change of purpose evidently predominates;
6. is necessary to prevent a security risk or other relevant public or ecclesiastical interests;
7. it is necessary in order to avoid the commission of crimes or administrative infractions, for its investigation, prosecution of those responsible, prosecution or execution of sentences;
8. is necessary to prevent a serious infringement of the rights of a third party,
9. it is necessary for scientific research, provided that the scientific interest is above the interest of the person affected by the change in the purpose of the processing and the purpose of the research could not be achieved in other ways, or only with a disproportionate effort;
10. is necessary for the performance of the functions proper to the Catholic Church or the powers entrusted to the ecclesiastical authorities,

§ 3. A new purpose for which data will be processed, that goes beyond the original purpose for which the data was collected, shall not be deemed incompatible if it takes place in the exercise of the powers of supervision and control, of audit, the execution of verifications by the processor, with the purpose of filing in the interest of the Catholic Church, for scientific or historical research purposes or for statistical purposes. This also applies to the processing for the purpose of training and control by the data controller, to the extent that this does not conflict with the interests of the data subject.

§4. If the processing for a purpose other than that for which personal data have been collected is not based on the consent of the person concerned or in an ecclesiastical or state rule, the processing shall only be lawful if the purpose of the new processing is compatible with the purpose for which the personal data were originally collected.

The controller shall consider whether the new purpose is "compatible" with the original purpose taking into account the following factors:

(a) any link between the original purpose and the new purpose;

(b) the context in which the data have been collected, including the controller's relationship with the data subjects;

(c) the nature of the personal data, in particular, whether special categories of personal data are affected;

(d) the possible consequences of the new purpose of processing for data subjects; and

(e) the existence of appropriate safeguards.

§ 5. Personal data that are only processed for control purposes, data backup or to ensure the proper functioning of a processing system can only be used for these purposes.

Article 7. Principles for the processing of personal data

§ 1. Personal data shall be:

1. processed in a lawful, fair and transparent manner in relation to the data subject ("lawfulness, loyalty and transparency");
2. collected for specific, explicit and legitimate purposes, and shall not be subsequently processed in a manner incompatible with said purposes, except as established in this General Decree or in the applicable regulations ("restriction of purpose");
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In particular, personal data must be pseudonymous to the extent that this is possible in accordance with the purpose for which they are used and that this is not disproportionate to the intended purpose of the protection ("data minimization");
4. exact and, if necessary, updated;
5. all reasonable measures shall be taken so that personal data that are inaccurate data with respect to the purposes for which they are processed ("accuracy") are removed or rectified without delay;
6. maintained in a way that allows the identification of the data subjects for no longer than necessary for the purposes of processing personal data, except as established in this General Decree or in the applicable regulations ("restriction of the term of retention");
7. processed in such a way as to ensure adequate security of personal data, including protection against unauthorized or illicit processing and against loss,

destruction or accidental damage, through the application of appropriate technical or organizational measures ("integrity and confidentiality")

§ 2. The data controller shall be responsible for complying with the provisions of § 1 of this Article and able to prove it ("proactive responsibility")

Article 8. Consent

§ 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

§ 2. If the consent is obtained from the data subject, the party is to be informed of the purpose of the processing and, if so required by the circumstances of the individual case or at the request of the data subject, of the consequences of the denial of consent. Consent is only valid if it is based on the free decision of the person concerned.

§ 3. Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

§ 4. If the consent of the data subject is given in the context of a written declaration that also refers to other matters, the request for consent shall be presented in a way that is clearly distinguished from the other matters, in an intelligible and easily accessible manner, and using a clear and simple language. Any part of a declaration, which constitutes a violation of this General Decree shall not be binding.

§5 To the extent that special categories of personal data are processed, the consent must also explicitly refer to such data.

§6. When the processing is based on the consent of the data subject, the processor must be able to show that party consented to the processing of one's personal data.

§ 7. The data subject shall have the right to withdraw one's consent at any time. The withdrawal of consent shall not affect the legality of the processing based on the consent prior to its withdrawal. Before giving consent, the data subject shall be informed of this right. It shall be as easy to withdraw the consent as it is to give it.

§ 8. When assessing whether consent is freely given, utmost 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.

§ 9. The personal data of a minor who receives online pastoral or other similar services from an ecclesiastical entity can only be processed if the child has reached the age of 16. If the minor has not yet reached the age of 16, the processing is only lawful if the consent was given or authorized by the holder of parental authority or

guardianship over the minor, and only to the extent that it was given or authorized. The data controller must, taking into account available technology, make reasonable efforts to guarantee, in such cases, that the consent has been granted or authorized by the person authorized to do so. If the child has reached the age of thirteen years and the pastoral service required is exclusively free pastoral counseling, offered by an ecclesiastical entity, the consent of the minor or the guardian is not required to process the personal data of the minor.

Article 9. Communication between ecclesiastical entities or ecclesiastical authorities

§ 1. The communication of personal data between ecclesiastical entities or ecclesiastical authorities is permitted if it is a consequence of compliance with a norm or is necessary for the fulfillment of its purposes and the requirements of the Article 6.

§ 2. The responsibility of the communication shall only be the addressee in those cases in which, by virtue of the applicable regulations, the data controller is obliged to communicate the data.

§ 3. The addressee can only process the data communicated for the purpose for which they have been communicated. Processing for other purposes is only permitted under the conditions of Article 6 § 2.

§ 4. §§ 1 to 3 shall also apply to communication to public authorities.

§ 5. If personal data that may be communicated in accordance with this paragraph are linked to other personal data, the data subject or a third party, in such a way that separation is impossible or only possible with an unreasonable effort, the communication shall be extended to such data as the interest of the communication reasonably justifies it, but the processing of the data linked by the recipient shall not be, by itself, admissible.

Article 10. Communication to non-ecclesiastical or public authorities

The communication of personal data to entities other than those included in the previous paragraph is only allowed if the requirements of Article 6 are met, the data controller has no legitimate interest in excluding such communication and it does not entail any danger to the mission of the Catholic Church.

Article 11. Processing of special categories of personal data

§ 1. The processing of special categories of personal data is prohibited.

§ 2. The prohibition in sub-article 1 does not apply if one of the following applies:

1. if the data subject has expressly consented to the processing of personal data for one or more specific purposes;

2. the processing is necessary for the purposees of carrying out the obligations and exercising specific rights of the controller or the data subject in the field of employment and social security and social protection law; and of employees falling directly under canon law;
3. if the processing is necessary to protect the vital interests of the data subject or of another natural person, in the event that the data subject is not physically or legally able to give his or her consent;
4. when the processing is carried out by a church entity or authority in the course of its legitimate activities and on the condition that the processing relates solely to the members or to former members or to persons who have regular contact or connection with its purposes and that the personal data are not disclosed outside the entity without the consent of the data subjects;
5. when the processing refers to personal data that the data subject has made manifestly public;
6. if the processing is necessary for the formulation, exercise or defense of judicial or administrative claims, or when the courts or the ecclesiastical authorities have to deal with the aforementioned data in the exercise of their respective jurisdictions;
7. if the processing is based on canon law, is proportional and legitimate to the objective pursued, respects the content of the right to data protection, and establishes appropriate and specific measures to safeguard the fundamental rights and interests of the data subject;
8. when the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, for medical diagnosis, the provision of health or social care, or for the management of systems and services in the field of health or social care on the basis of canon law or state law, or under contract with a health professional and subject to the conditions and guarantees mentioned in § 3;
9. if the processing is appropriate and specific for reasons of public interest in the field of public health or to guarantee high quality and safety standards for health care and for medicines and medical devices, based on ecclesiastical or national legislation. In such a case, necessary measures are foreseen to protect the rights and freedoms of the person concerned, in particular professional secrecy;
10. The processing is necessary for archiving purposes in the interest of the Catholic Church, scientific or historical research purposes or statistical purposes, is based on canon law, is proportional to the objective pursued, preserves the essence of the right to privacy and establishes appropriate and specific measures to safeguard the fundamental rights and interests of the data subject.

§ 3. Special categories of personal data may be used in accordance with sub-article 2,8, of the previous paragraph, if they are processed by or under the responsibility of a professional subject to the obligation of profesional secrecy, or if the processing is carried out by another person who is subject to an obligation of confidentiality under the applicable law.

§ 4. In cases where the prohibition of processing is not applicable, the data controller, taking into account the state of the technology, the costs of implementation and the nature, scope, circumstances and purposes of the processing and the probability and severity of the risks to the rights and freedoms associated with the processing, shall provide the natural persons appropriate and specific measures to safeguard the interests of the data subject.

Article 12. Processing of personal data relating to convictions and criminal offenses

The processing of personal data relating to convictions and criminal offenses or related security measures in accordance with Article 6 § 1, may only be carried out when allowed by canon law or state law, and adequate guarantees are established for the rights and freedoms of the data subjects.

Article 13. Processing that does not require identification

§ 1. If the purposes for which a controller deals with personal data do not require or no longer require the identification of a data subject by the data controller, the latter shall not be obliged to maintain, obtain or process additional information in order to identify the data subject with the only purpose of complying with this General Decree.

§ 2. If the controller is capable of demonstrating that he/she is not in a position to identify the data subject, he/she shall inform the data subject accordingly, if possible. In these cases, Articles 17 to 22 shall not apply, unless the data subject provides additional information that allows him to exercise his rights under those provisions.

§ 3. An identity document shall only be processed when such processing is clearly justified having regard to the purpose of the processing and:
(a) the importance of secure identification; or
(b) any other valid reason as may be provided by law:

Provided that the national identity number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this General Decree,

Chapter III

Obligations of information of the data controller and rights of the data subject

Section 1
Obligations concerning information by the data controller

Article 14. Transparency of information and methods of exercising the rights of the data subject

§ 1. The data controller shall take the necessary measures to provide the data subject within a reasonable time, with all the information indicated in Articles 15 and 16, as well as any communication in accordance with Articles 17 to 24 and 34, regarding the processing, in a concise, transparent, intelligible and easily accessible manner, with a clear and simple language, in particular any information specifically aimed at a minor. The information shall be provided in writing or by other means, including, if applicable, by electronic means. When requested by the data subject, the

information may be provided orally provided that the identity of the data subject is demonstrated by other means.

§ 2. The controller shall facilitate the exercise of data subject rights under under Articles 17 to 24.

§ 3. In the case of Article 13 § 2, the data controller shall not refuse to act on the request of the data subject in the exercise his rights under Articles 17 to 24, unless he can demonstrate that he is not in a position to identify to the data subject.

§ 4. The data controller shall provide the data subject with information relating to their actions on the basis of an application in accordance with Articles 17 to 24, and, in any case, within one month of receipt of the request. This period may be extended for another two months if necessary, taking into account the complexity and the number of applications. The controller shall inform the data subject of any such extension within one month of receiving the request, indicating the reasons for the delay. When the data subject submits the application by electronic means, the information shall be provided by electronic means whenever possible, unless the data subject requests that it be provided otherwise.

§ 5. If the controller does not comply with the request of the data subject, he/she shall inform it without delay, and no later than one month after receiving the request, the reasons for not acting and the possibility of submitting a claim before the Supervisory and seeking a judicial remedy.

§ 6. The information provided under Articles 15 and 16, as well as any communication and any action taken under Articles 17 to 24 and 34, shall be free of charge. When the requests are manifestly unfounded or excessive, especially due to their repetitive nature, the data controller may:
1. charge a reasonable fee based on the administrative costs incurred to provide the information or communication or perform the requested action, or
2. Refuse to act on the application.

§ 7. The data controller shall bear the burden of demonstrating the manifestly unfounded or excessive nature of the request.

§ 8. Without prejudice to the provisions of Article 13, when the data controller has reasonable doubts regarding the identity of the natural person who is making the request referred to in Articles 17 to 23, the controller may request the additional information necessary to confirm the identity of the data subject.

Article 15. Information to be provided where personal data are collected from the data subject

§ 1. Where personal data relating to a data subject are collected from the data subject, the Controller shall, at the time when the personal data are obtained, provide the data subject with all the following information:

1. the identity and contact details of the data controller;

2. contact information of data protection officer/s, if applicable;
3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing in accordance with Article 6 of this General Decree;
4. when the processing is based on Article 6 § 1.7, the legitimate interests of the data controller or of a third party;
5. where applicable, the recipients or the categories of recipients of the personal data, if any;
6. where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the EU Commission, or, in the case of transfers in accordance with Article 40, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

§ 2. In addition to the information mentioned in § 1 of this Article, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

1. the period for which the personal data shall be stored or, if that is not posible, the criteria used to determine this term;
2. the existence of the right to request from the controller access to personal data relating to the data subject, and its rectification or suppression, or the restriction of its processing, or to oppose the processing, as well as the right to the portability of the data, in accordance with Articles 17-20 and 22-23 of this General Decree;
3. when the processing is based on Articles 6 § 1.2 or 11 § 2, 1), the existence of the right to withdraw consent, in accordance with Article 8, § 6 of this General Decree, at any time, without affecting to the legality of the processing based on the consent prior to its withdrawal;
4. the right to lodge a complaint with a Supervisory Authority;
5. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
6. the existence of automated decision-making, including profiling, referred to in Article 24 §§ 1 and 4, and, at least in such cases, significant information on the logic applied, as well as the importance and expected consequences of said processing for the data subject.

§ 3. Where the data controller intends to process the personal data for a purpose other than that for which they were collected, the controller shall inform the data subject of the new purpose of the processing and of the relevant aspects thereof.

§ 4. The foregoing shall not apply as long as the data subject already has the information or an effort disproportionate to the interest of the affected person is required; and, in any case, if in the context in which the data are collected, the information would be inconsequential.

§ 5. Nor shall it apply:

1. when the data or the fact of its storage or processing must be kept secret by virtue of the provisions of this General Decree, by canon law or other applicable regulations;
2. when there are other protected rights or interests, including those of the data controller, that must prevail over the obtaining of the information by the data subject.
3. if the provision of information may jeopardize the performance of the functions proper to the Catholic Church or the powers entrusted to the ecclesiastical authorities.

Article 16. Information to be provided when personal data has not been obtained from the data subject

§ 1. When the personal data has not been obtained from the data subject, the data controller shall provide the information specified in Article 15 §§ 1 and 2, and, in addition:

1. the categories of personal data concerned;
2. the source of the personal data and, where appropriate, if they come from sources of public access,

§ 2. The controller shall provide the information indicated in §§ 1 and 2 of Article 15:
1. within a reasonable time, after obtaining the personal data, but at thte lastest within one month, having regard to the specific circumstances in which the personal data are processed;
2. if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject, or
3. if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

§ 3. When the controller plans the further processing of the personal data for a purpose other than the one for which they were obtained, the controller shall provide the data subject, prior to that further processing, with information on that other purpose and with any relevant information indicated in § 1 of this Article.

§ 4. The provisions of §§ 1 to 3 of this Article shall not be applicable where and insofar as:

1. the data subject already has the information;
2. the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving in the interest of the Catholic Church, scientific or historical research purposes or statistical purposes, to the extent that the obligation mentioned in the § 1 of this Article may seriously impede or hinder the achievement of the objectives of such processing. In such cases, the data controller shall adopt adequate measures to protect the rights, freedoms and legitimate interests of the data subject, including making the information publicly available;

3. the obtaining or communication is expressly established by this General Decree, by canon law or other applicable regulations and appropriate measures are taken to protect the legitimate interests of the data subject, or
4. where personal data are subject to the obligation of secrecy or confidentiality in accordance with canon law or other regulations and therefore must be treated confidentially.

§ 5. Sections 1 to 3 of this Article shall not apply if providing the information supposes:
1. jeopardize the performance of the functions proper to the Catholic Church or the powers entrusted to the ecclesiastical authorities;
2. injure other rights or protected interests that must prevail over the obtaining of the information by the data subject.

§ 6. If the information provided in § 1 is not provided to the data subject, the controller shall take the appropriate measures to protect the legitimate interests of the data subject and must record in writing the cause for which he refrained from providing the information.

Section 2
Rights of the data subject

Article 17. Right of access by the data subject

§ 1. The data subject shall have the right to obtain from the data controller the confirmation of whether or not personal data concerning him or her are being processed and, in such case, the right to access personal data and the following information:
1. the purposes of processing;
2. the categories of personal data concerned;
3. the recipients or categories of recipients to whom the personal data were communicated or will be communicated, in particular, recipients in third countries or international organizations;
4. where possible, the expected period of retention of personal data or, if this is not possible, the criteria used to determine this period;
5. the existence of the right to request from the data controller the rectification or deletion of personal data or the restriction of the processing of personal data relating to the data subject, or to oppose such processing, in accordance with Articles 18, 19, 20 and 23 of this Decree General;
6. the right to file a claim with the supervisory authority;
7. any information available about its origin, when the personal data has not been obtained from the data subject;
8. the existence of automated decisions, including profiling, referred to in Article 24, §§ 1 and 4, and, at least, in such cases, significant information on the logic applied, as well as the importance and expected consequences of such processing for the data subject

§ 2. When personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate guarantees under Article 40, relating to the transfer.

§ 3. The data controller shall provide a copy of the personal data that is being processed. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. When the data subject submits the application by electronic means, and unless the latter requests that it be provided otherwise, the information shall be provided in a commonly used electronic format.

§ 4. The right to obtain a copy mentioned in the previous section shall not negatively affect the rights and freedoms of others.

§ 5. There shall not be this right of access, if it is not possible to identify the person, or where the necessary information is not provided, or the administrative costs to allow such identification are not reasonable. In addition, this right of access of the data subject shall not exist if:
1. the data subject should not be informed, in accordance with Articles 15 and 16; or
2. the data:
(a) is merely stored because it cannot be deleted under the provisions of this General Decree, canon law or other applicable regulations, or
(b) is stored only for data protection or privacy control purposes, the provision of information would require a disproportionate effort and processing for other purposes would be excluded by appropriate technical and organizational measures.

§ 6. The reasons for the denial of the information must be documented and justified to the data subject, unless the communication of the justification jeopardizes the purpose pursued by the denial of the information. The data stored for the purpose of preparing and providing information to the data subject, can only be processed for this purpose and for data protection purposes; for other purposes, processing in accordance with Article 20, must be restricted.

§ 7. If the access request is made by or through an ecclesiastical entity, the information denied must be brought to the attention of the competent Data Protection Officer, so that he can analyze the elements of the legality of the denial, except that the competent ecclesiastical authority considers that this communication would seriously affect the interests of the Catholic Church.

Article 18. Right of rectification

§ 1. The data subject shall have the right to obtain from the data controller, without undue delay, the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have personal data that are incomplete corrected, including by means of an additional declaration.

§ 2. The right of rectification does not apply if the personal data is stored for archival purposes in the interest of the Catholic Church, scientific or historical research purposes or statistical purposes. If the data subject questions the accuracy

of the personal data, the uncorrected data may not be processed for purposes other than archival purposes in the interest of the Catholic Church, scientific or historical research purposes or statistical purposes and, if these purposes are not put at risk, the request for rectification of the data subject may be recorded.

Article 19. Right of Withdrawal of Consent and Erasure of Data

§ 1. The data subject shall have the right to obtain from the data controller, without undue delay, the deletion of personal data concerning him, provided that any of the following circumstances:

1. Personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
2. the data subject withdraws the consent on which the processing is based in accordance with Article 6 § 1.2, or Article 11 § 2.1, and where there is no other legal ground for the processing;
3. the data subject objects to the processing under Article 23 § 1, and no other legitimate grounds for the processing prevail, or the data subject objects to the processing under Article 23 § 2;
4. personal data have been processed illicitly;
5. the personal data must be deleted for the fulfillment of a legal obligation established in this General Decree or in another norm of canon law;
6. the personal data have been collected in relation to the offer of information society services referred to in Article 8.

§ 2. Where the personal data are made public, and the controller is obliged, by virtue of the provisions of section 1, to delete such data, the data controller, taking account of available technology and the cost of its application, shall take reasonable measures, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the deletion by such cotrollers of any links to, or copy or replication of, those personal data.

§ 3. §§ 1 and 2 of this Article shall not apply when the processing is necessary:

1. to exercise the right to freedom of expression and information;
2. for the compliance with a legal obligation that requires the processing of data imposed in this General Decree, in canon law or in other regulations applicable to the data controller, or for the performance of the proper functions of the Catholic Church or the powers entrusted to it to the ecclesiastical authorities,
3. for reasons of public interest in the field of public health in accordance with Article 11 § 2.8 and 9 and Article 11 § 3; or
4. archival purposes in the interest of the Catholic Church, scientific or historical research purposes or statistical purposes, to the extent that the right indicated in section 1 could make it impossible or seriously impede the achievement of the objectives of such processing, or
5. for the formulation, exercise or defense of legal claims.

§ 4. If the elimination is not possible or only possible at a disproportionately high cost, due to the special nature of the storage, the right of deletion is replaced by the right to restriction of processing, in accordance with Article 20. The blocking of the data is also applied as a restriction of the processing.

Article 20. Right to restriction of processing

§ 1. The data subject shall have the right to obtain from the data controller the restriction of the processing of the data where one of the following applies:
1. the data subject challenges the accuracy of the personal data, during a period that allows the controller to verify the accuracy of the same;
2. the processing is unlawful and the data subject opposes the deletion of personal data and requests instead the restriction of its use;
3. the controller no longer needs the personal data for the purposes of the processing, but the data subject needs them for the establishment, exercise or defense of legal claims;
4. the data subject has objected to the processing, under Article 23, pending the verification whether the legitimate grounds of the controller override those of the data subject.

§ 2. When the processing of personal data has been limited by virtue of section 1, the data shall, with the exception of storage, only be processed with the data subject's consent, or for the establishment, exercise or defence of legal claims or for the protection of the rights of antoher natural or legal persono or for reasons of important ecclesiastical interest.

§ 3. Any data subject who has obtained the restriction of processing in accordance with paragraph 1 shall be informed by data controller before the restriction of processing is lifted.

§ 4. The provisions of § 1.1 to 3 shall not apply in the cases outlined in the Article 19 § 3.

Article 21. Obligation to notify regarding the rectification or deletion of personal data or the restriction of processing.

The data controller shall communicate any rectification or deletion of personal data or restriction of processing, carried out in accordance with Articles 18, 19 §§ 1 and 20, to each of the recipients to whom the personal data have been communicated, unless it is impossible or requires a disproportionate effort. The processor shall inform the data subject about those recipients, if the data subject requests it.

Article 22. Right to the portability of the data

§ 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a data controller, in a structured, commonly used and machine-readable format, and have the right to transmit those data to antoher controller without hindrance from the controller to which the personal data have been provided where:

1. the processing is based on the consent, in accordance with the contract in accordance with Article 6 § 1.3, and
2. the processing is carried out by automated means.

§ 2. In exercising one's right to data portability, in accordance with the foregoing, the data subject shall have the right to have personal data transmitted directly from a data controller to another, where this is technically feasible.

§ 3. The exercise of the right mentioned in § 1 of this Article shall be without prejudice to Article 19. That right shall not apply to the processing necessary for the performance of the functions proper to the Catholic Church or the powers entrusted to the ecclesiastical authorities.

§ 4. The right mentioned in § 1 of this Article shall not adversely affect the rights and freedoms of others.

§ 5. The right to portability of data shall also not apply when there are archiving purposes in the interest of the Church Catholic, scientific or historical research purposes or statistical purposes, to the extent that the right indicated in § 1 of this Article could make it impossible or seriously impede the achievement of the objectives of such processing.

Article 23. Right to object

§ 1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any tie to processing of personal data concerning him or her which is based on the provisions of Article 6 § 1.6 or 7, including profiling based on these provisions. The data controller shall stop processing personal data, unless:

1. the controller demontrates compelling legitimate grounds that prevail over the interests, rights and freedoms of the data subject;
2. it is necessary for the establishment, exercise or defense of legal claims:
3. it is necessary for the realization of the proper functions of the Catholic Church or of the powers entrusted to the ecclesiastical authorities:
4. is necessary for the fulfillment of a legal obligation imposed in this General Decree, in canon law or in other applicable regulations.

§ 2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

§ 3. When the data subject opposes the processing for the purpose of direct marketing, personal data shall no longer be processed for such purposes.

§ 4. At the latest at the time of the first communication with the data subject, the right referred to in §§ 1 and 2 of this Article shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately of any other information.

§ 5. When personal data is processed, in the interest of the Catholic Church, for purposes of scientific or historical research purposes, or for statistical purposes, the data subject shall have the right, on grounds relating to his/her particular situation, to object to the processing of personal data concerning him/her, unless the

processing is necessary for the performance of the functions proper to the Catholic Church or the powers entrusted to the ecclesiastical authorities.

Article 24. Automated individual decision-making, including profiling

§ 1. The data subject shall have the right not to be the subject of a decision based solely on automated processing, including profiling, which produces legal effects on him or her or similarly significantly affects him or her.

§ 2. § 1 of this Article shall not apply if the decision:

1. is necessary for the conclusion or execution of a contract between the data subject and the data controller;
2. is admissible by virtue of what is established in this General Decree, in canon law or in other applicable legislation and also adequate measures are established to safeguard the rights and liberties and legitimate interests of the data subject;
3. is based on the explicit consent of the data subject;
4. is necessary for the performance of the functions proper to the Catholic Church or the powers entrusted to the ecclesiastical authorities.

§ 3. In the cases referred to in § 2.1 and 3, the data controller shall take the appropriate measures to safeguard the rights and freedoms and the legitimate interests of the person concerned.

§ 4. The decisions referred to in § 2 of this Article shall not be based on the special categories of personal data referred to in Article 11 § 1, unless the Article 11 § 2.1 or 7 is applies, and appropriate measures have been taken to safeguard the rights and freedoms and legitimate interests of the person concerned.

Article 25. Provisions common to the rights of the data subject

§ 1. The rights regulated in this section may only be excluded or restricted by virtue of what is established in this General Decree, in canon law or in other applicable regulations.

§ 2. If the data of the data subject is stored automatically in such a way that there are several controllers, the data subject can go to each one of them to exercise his/her rights, the data controller shall transfer the request of the data subject to the competent entity and report that transfer to the data subject.

Chapter IV

Controller and Processor

Section 1
Technology and organization; processing of work

Article 26. Technical and organizational measures

§ 1. Taking into account, among others, the state of the technology, the costs of execution, the nature, scope, context and purposes of the processing, as well as the risks of various probability and risks for the rights and freedoms of natural persons, the controller and the processor shall apply appropriate technical and organizational measures in order to guarantee and be able to demonstrate that the processing is in accordance with this General Decree and applicable regulations. These measures include, among others:

1. the use of pseudonyms, the unlinking of identity and the encryption of personal data, where appropriate;
2. the ability to guarantee the permanent confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore availability and access to personal data quickly in the event of a physical or technical incident;
4. a process of regular verification, assessment and assessment of the effectiveness of technical and organizational measures to ensure the safety of the processing.

§ 2. When evaluating the adequacy of the security level, the risks presented by data processing shall be taken into account, in particular as a result of the accidental or unlawful destruction, loss or alteration of personal data transmitted, conserved or otherwise processed, or unauthorized communication or access to said data.

§ 3. Measures shall only be necessary if the effort in their implementation is in reasonable proportion to the purpose of protection.

§ 4. Adherence to approved codes of conduct in accordance with the provisions of Article 46 may be used as an element to demonstrate compliance with the obligations set out in § 1 of this Article.
§ 5. The controller and the processor shall take measures to guarantee that any person acting under the authority of the controller or the processor and having access to personal data may only process such data in accordance with the instructions of the controller, unless it is necessary by virtue of this General Decree, canon law or other applicable regulations.

Article 27. Data Protection by design and by default

§ 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate

technical and organisational measures, such as the use of pseudonyms, designed to apply effective form of data protection principles, such as data minimization, and integrate the necessary guarantees in the processing, in order to comply with the requirements of this General Decree and protect the rights of the interested parties.

§ 2. The Data controller shall apply the appropriate technical and organizational measures with a view to ensuring that, by default, only the personal data necessary for each of the specific purpose of the processing are processed. That obligation shall apply to the amount of personal data collected, the extent of its processing, its term of retention and its accessibility. Such measures shall ensure in particular that, by default, personal data are not accessible, without the intervention of the person, to an indeterminate number of natural persons.

Article 28. Joint Controllers

§ 1. Where two or more controllers jointly determine the objectives and the means of processing, shall be joint controllers. The controllers shall determine in a transparent and mutually agreed manner their respective responsibilities in fulfilling the obligations imposed by Canon Law and/or this General Decree or, in particular, in the exercise of the rights of the data subject and their respective obligations to supply of information, referred to in Articles 15 and 16, except, and insofar that, their respective responsibilities are governed by peremptory norms of law. Such agreement may designate a point of contact for the interested parties.

§ 2. The agreement indicated in § 1 of this Article shall duly reflect the respective roles and relationships of the joint controllers in relation to the interested parties. The essential aspects of the agreement shall be made available to the data subject.

§ 3. Regardless of the terms of the agreement referred to in § 1 of this Article, the data subject may exercise the rights recognized by this Decree in respect of and against each of the controllers.

Article 29. Processors

§ 1. Where processing is to be carried out on behalf of a data controller, the controller shall choose only a processor who guarantees to apply appropriate technical and organizational measures, so that the processing is in accordance with the requirements of this General Decree and ensure the protection of the rights of the data subject.

§ 2. The processor shall not engage another processor without the prior written, specific or general authorization of the controller. In the latter case, the processor shall inform the controller of any change foreseen in the addition or substitution of other processors, giving the controller the opportunity to object to such changes.

§ 3. The processing by a processor shall be governed by a contract, or other legal act under Canon Law or the Regulations, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of

data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

1. processes the personal data only following the documented instructions of the controller, including with respect to the transfer of personal data to a third country or an international organization, unless it is obliged to this by virtue of this General Decree, canon law or other regulations applicable to the processor; in such case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits it;
2. ensures that persons authorized to process personal data have undertaken to respect confidentiality or are subject to an obligation of confidentiality of a statutory or legal nature;
3. shall take all necessary measures in accordance with Article 26;
4. shall respect the conditions indicated in §§ 2 and 5 of this Article to resort to another processor;
5. assists the controller, taking into account the nature of the processing, through appropriate technical and organizational measures, whenever possible, so that it can meet his obligation to respond to requests that are intended to exercise the rights of those concerned established in chapter III;
6. must assist the controllers to comply with the obligations set out in Articles 33 to 35, taking into account the nature of the processing and the information at their disposal;
7. at the discretion of the controller, he shall delete or return all the personal data once the rendering of the processing services ends, and he shall delete the existing copies, unless the conservation of the personal data is required by virtue of this General Decree, of the Canonical Law or of other applicable regulations;
8. makes available to the controller all the necessary information to demonstrate compliance with the obligations established in this Article, as well as to allow and contribute to the performance of audits, including inspections, by the controller or by another auditor authorized by the same. The processor shall immediately inform the data controller if, in his opinion, an instruction violates this General Decree, canon law or any other applicable regulation.

§ 4. Where a processor engages another processor to carry out specific processing activities on behalf of the controller, the same data protection obligations as stipulated in the contract or other act legal between the processor and the processor referred to in § 3 of this Article shall be imposed on this other processor, by a contract or other legal act under Canon Law or the Regulations, that is binding on the processor, in particular the provision of sufficient guarantees of application of appropriate technical and organizational measures, so that the processing is in accordance with the provisions of this Decree. If that other processor fails to comply with their data protection obligations, the initial processor shall continue to respond to the data controller, as regards compliance with the obligations of the other processor

§ 5. The adherence of the processor to approved codes of conduct in accordance with the provisions of Article 46, may be used as an element to demonstrate the existence of sufficient guarantees referred to in §§ 1 and 4 of this Article.

§ 6. Without prejudice to an individual contract between the controller and the processor, the contract or other legal act referred to in §§ 3 and 4 of this Article may be based, in whole or in part, on the standard contractual clauses referred to in § 7 of the same Article, including when they form part of a certification granted to the processor or in charge.

§ 7. The competent Data Protection Officer may establish contractual clauses type for the issues referred to in §§ 3 to 5 of this Article.

§ 8. The contract or other legal act referred to in §§ 3 and 4 of this Article shall be in writing, including in electronic format.

§ 9. If a processor infringes the present General Decree by determining the purposes and means of the processing, the processor shall be considered to be a controller in respect of that processing.

Article 30. Processing under the authority of the controller or the processor

The processor of data and any person acting under the authority the controller or of the processor, who have access to personal data shall not process those data except on instructions from the controller, unless required to do so by virtue of this General Decree, Canon Law or other applicable regulations.

Section 2
Obligations of the controller

Article 31. Record of processing activities

§ 1. Every controller and, where applicable, his representative, shall keep a record of the processing activities carried out under his responsibility. This register shall contain the following information:

1. the name and contact information of data controller and, where applicable, the joint controller, and the data protection officer;
2. the purposes of processing;
3. a description of the categories of data subjects and the categories of personal data;
4. the use of profiles, where applicable;
5. the categories of recipients to whom the personal data were communicated or will be communicated, including the recipients in third countries or international organizations;
6. where possible, transfers of personal data to a third country or an international organization, including the identification of such third country or international organization and, in the case of the transfers indicated in Article 41.2, the documentation of adequate guarantees;
7. where possible, the deadlines for the deletion of different categories of data;
8. whenever possible, a general description of the technical and organizational security measures referred to in Article 26.

§ 2. Each processor shall keep a record of all the categories of processing activities carried out on behalf of the controller which shall contain:

1. the name and contact information of the processor or those in charge and of each controller for which the processor acts, and of the data protection officer;
2. the categories of processing carried out on behalf of each controller;
3. where applicable, the transfer of personal data to a third country or international organization, including the identification of said third country or international organization and, in the case of the transfers indicated in Article 41.2, the documentation of adequate guarantees;
4. whenever possible, a general description of the technical and organizational security measures referred to in Article 26.

§ 3. The records referred to in §§ 1 and 2 of this Article shall be in writing.

§ 4. Data controller or the processor shall make the register available to the competent data protection officer and the supervisory authority on request.

§ 5. The obligations set forth in §§ 1 and 2 of this Article shall not apply to any company or organization employing less than 250 persons, unless the processing performed may entail a risk to the rights and freedoms of the interested parties, is not occasional, or includes special categories of personal data indicated in Article 11, or personal data relating to convictions and criminal offenses refers to Article 12.

Article 32. Cooperation with the supervisory authority and the Data Protection Officer

The controller and the processor shall cooperate with the supervisory authority as well as with the competent Data Protection Officer/s, upon request and, always, under the coordination of the designated Lead Data Protection Officer/s of the Archdiocese of Malta.

Article 33. Notification of a personal data breach to the supervisory authority

§ 1. In case of a personal data breach, the controller shall notify the competent supervisory authority, through the relevant Data Protection Officer and the Archdiocese of Malta, without undue delay and, where feasible, not later tan 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, itmust include the reasons for the delay.

§ 2. The data processor shall notify the controller without undue delay after becoming aware of a personal data breach.

§ 3. The notification referred to in § 1 of this Article shall, at least:

1. describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects affected, as well as the categories and approximate number of personal data records affected;
2. communicate the name and contact details of the data protection officer;
3. describe the likely consequences of the personal data breach;
4. describe the measures adopted or proposed by the data controller to remedy the breach of the security of personal data, including, if applicable, the measures adopted to mitigate the possible negative effects.
5. The information shall be provided gradually and without undue delay, when it is not possible to provide it at the same time.
6. The controller shall document any breach of the security of personal data, including the facts related to it, its effects and the corrective measures adopted. This documentation shall allow the control authority to verify compliance with the provisions of this Article.

Article 34. Communication of a personal data breach to the data subject

§ 1. When the personal data break is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without delay.

§ 2. The communication to the data subject contemplated in § 1 of this Article shall describe in clear and simple language the nature of the personal data breach and shall contain at least the information as well as the measures referred to in the Article 33 § 3.2-4.

§ 3. The communication to the data subject referred to in § 1 shall not be necessary if one of the following conditions is met:

1. that the data controller has adopted appropriate technical and organizational protection measures, and these measures have been applied to the personal data affected by the breach, particularly those encryption measures, which render the personal data unintelligible to anyone who does not have authorization to access them;
2. that data controller has taken further steps aimed at reducing, as far as possible, the high risk to the rights and freedoms of the data subject, referred to in § 1 of this Article;
3. it would involve disproportionate effort. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

§ 4. When the processor has not yet informed the data subject of the violation of the security of the personal data, the supervisory authority, once considered the likelihood that such a violation entails a high risk, may require it to do so or may decide that any of the conditions mentioned in § 3 of this Article is met.

Article 35. Data protection impact assessment and prior consultation

§ 1. Where a type of processing in particular using new technologies and taking in to account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall prior to the processing carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessmnet may address a set of similar processing operations that present similar high risks.

§ 2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

§ 3. The controller can ask the Data Protection Officer of the Archdiocese of Malta, about the appropriateness of consulting the control authority.

§ 4. The relative data protection impact assessment referred to in § 1 of this Article shall be required in case of:

1. systematic and exhaustive evaluation of personal aspects of natural persons, based on an automated processing, such as profiling, and on the basis of which decisions are taken that produce legal effects for natural persons or that significantly affect them in a similar way;
2. large-scale processing of the special categories of data referred to in Article 11, or of personal data relating to convictions and criminal offenses, referred to in Article 12; and
3. large-scale systematic observation of a public access area.

§ 5. The Data Protection Officers may also, within their area of competence, establish and publish the list of types of processing that require data protection impact assessment.

§ 6. The Data Protection Officers shall coordinate, within their scope of competence, and through the Data Protection Officer of the Archdiocese, the lists of the types of processing that require data protection impact assessment.

§ 7. The impact assessment shall contain at least:

1. a systematic description of the planned processing operations and their purposes, including, where applicable, the legitimate interest pursued by the controller;
2. an assessment of the necessity and proportionality of processing operations with respect to their purpose;
3. an assessment of the risks to the rights and freedoms of the interested parties in accordance with § 1 of this Article; and
4. the measures provided to address the risks, including guarantees, security measures and mechanisms that guarantee the protection of personal data, as well as measures to demonstrate compliance with this General Decree, taking into account the legitimate rights and interests of the interested parties and other affected people.

§ 8. The compliance with the codes of conduct, referred to in Article 46, by the controllers or processors, shall be duly taken into account when evaluating the repercussions of the processing operations carried out by those controllers or processors, in particular for purposes of the data protection impact assessment.

§ 9. The data controller shall obtain, as applicable, the opinion of the data subjects or their representatives in relation to the planned processing, without prejudice to the protection of ecclesiastical interests or of the security of the processing operations.

§ 10. When the processing in accordance with Article 6 § 1.4 or 6, has its legal basis in this General Decree, in canon law or in other regulations that apply to data controller, §§ 1 to 7 shall not be applicable, unless the rule containing the obligation establishes the need to proceed with such an assessment prior to the processing activities.

§ 11. The controller shall review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

§ 12. The processor, through the Data Protection Officer of the Archdiocese of Malta, shall consult the supervisory authority before proceeding to the processing, where a data protection impact assessment under this Article indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate that risk.

Section 3
Data Protection Officer

Article 36. Designation of data protection officer

§ 1. An officer for Data Protection shall be appointed by:

1. The Diocese of Gozo;
2. The entities mentioned in Article 3, of a canonical public nature;
3. The entities cited in Article 3, of a private canonical nature, in cases where it is mandatory.

§ 2. The Data Protection Officer referred to in § 1 of this Article, shall act within the competence of the entity that appoints him.

§ 3. The scope of competence of the Data Protection Officers referred to in § 1.2 of this Article, shall be that of the entity that has appointed them, without prejudice to the powers of the Data Protection Officers referred to in paragraphs 1 thereof.

§ 4. Data Protection Officers shall be appointed:

1. In the Diocese Church, the Moderator of Curia, according to canon 473 § 2 and in accordance with the Code of Canon Law, or the person designated by the competent ecclesiastical authority, must meet at least the requirements of the following point.

2. In the entities of § 1.2 of this Article, the data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices.

§ 5. In the entities of § 1.3 of this Article, the person designated by the entity itself, communicating the name of the appointee to the competent ecclesiastical authority.

§ 6. The competent ecclesiastical authority shall provide, where applicable, the designated Data Protection Officer, the means for their formation in the matter as well as the due advice of professionals with specialized knowledge of the Law and in terms of data protection.

§ 7. The Data Protection Officer cannot be responsible for any area in terms of data protection.

§ 8. The controller or the processor shall publish the contact data of the data protection officer and shall communicate them to the supervisory authority.

§ 9. A single Data Protection Officer can be appointed for the entities of §§ 1.2 and 3, when authorized by the competent ecclesiastical authority.

Article 37. Position of data protection officer

§ 1. The controller shall ensure that the data protection officer is involved properly and in a timely manner in all issues relating to the protection of personal data.

§ 2. The Data controller shall support the data protection officer in the performance of the functions mentioned in Article 38, providing the necessary resources for the performance of those functions and access to personal data, as well as to the processing operations, and to maintain his or her expert knowledge.

§ 3. The controller shall ensure that the data protection officer does not receive any instructions that prevent him from performing his duties. The Data Protection Officer cannot be dismissed or be punished for performing his duties and shall report directly to the highest hierarchical level of the controller.

§ 4. The data protection officer shall be obliged to maintain secrecy or confidentiality with regard to the performance of his duties.

§ 5. The data protection officer may perform other functions and tasks. The data controller shall ensure that these functions and tasks do not result in a conflict of interest and are not so extensive as to prevent him from fulfilling his obligations under this General Decree or other norms of Canon Law.

§ 6. The data subjects may make contact with the data protection officer in relation to all matters relating to the processing of their personal data and the exercise of their rights, under the present General Decree, at any time and, in any case, before going to the independent supervisory authority.

Article 38. Tasks of the data protection officer

§ 1. The data protection officer shall have at least the following tasks:

1. to inform and advise the controller, the processor and the employees that carry out data processing within the scope of their respective competence;
2. to monitor compliance with this General Decree and other applicable personal data protection regulations, as well as the policies of data controller or the data processor in charge of personal data protection, including assignment of responsibilities, awareness-raising and training of personnel involved in the processing operations, and the related audits;
3. to provide the advice where requested as regards the data protection impact assessment and supervise its application in accordance with Article 35;
4. to cooperate with the supervisory authority through the Data Protection Officer of the Archdiocese of Malta, which shall act as the contact point of the supervisory authority for matters relating to the processing, including the prior consultation referred to in Article 35, and perform consultations, where appropriate, on any other matter;
5. Other functions as established in this General Decree.

§ 2. The data protection delegate shall in the performance of his/her duties have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of the processing.

Chapter V

Transfer of personal data to third countries or international organizations

Article 39. General principles

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of, the present General Decree, the conditions laid down in this chapter are complied with by controller and the processor, including those related to the subsequent transfers of personal data from the third country or international organization to another third country or another international organization. Transfers of personal data between ecclesiastical authorities shall not be considered transfers of personal data to third countries or international organizations.

The Catholic Church and its entities, according to art. 3.1 of this General Decree, enjoy the freedom to maintain relations and communicate with the Holy See, the Episcopal Conferences, the particular Churches, as well as between them and with other communities, institutions, organizations and individuals, in Malta or in a third country; no provision of this General Decree can be interpreted in a manner that significantly limits this freedom.

Article 40. Transfers on the basis of an adequacy decision

§ 1. A transfer of personal data to a third country or international organization may be carried out if, according to the opinion of the Data Protection Officer of the Archdiocese of Malta, there is a guarantee of an adequate level of protection.

§ 2. If a decision on adequacy is not available by virtue of the foregoing, personal data may be transferred if:
1. a legally binding instrument establishes adequate safeguards for the protection of personal data, or
2. The data controller, having evaluated all the circumstances involved in the transfer, can assume that there are adequate safeguards for the protection of personal data and so documents it.

Article 41. Exceptions

In the absence of the requirements of the previous paragraph, transfers of personal data to a third country or international organization shall only be carried out if one of the following conditions is met:

1. that the data subject has explicitly given his consent to the proposed transfer, after having been informed of the possible risks, if any;
2. that the transfer is necessary for the execution of a contract between the data subject and the data controller or for the execution of pre-contractual measures adopted at the request of the data subject;
3. that the transfer is necessary for the execution of a contract, in the interest of the data subject, between the data controller and another natural or legal person;
4. that the transfer is necessary according to the juridical order of the Catholic Church.
5. that the transfer is necessary for the formulation, exercise or defense of claims;
6. that the transfer is necessary to protect the vital interests of the data subject or of other persons, when the data subject is physically or legally incapable of giving his or her consent.

Chapter VI

Data Protection Supervisory Authority

Article 42. Data protection Supervisory Authority

§ 1. The Catholic Church in Malta/Gozo reserves the right to establish, in the future, in accordance with the regulations in force, a specific independent supervisory authority.

§ 2. Any communication between the entities referred to in Article 3 of this General Decree and the competent Supervisory Authority must necessarily be carried out through the Data Protection Officer of the Archdiocese of Malta.

Chapter VI

Other provisions

Article 43. Video surveillance

§ 1. The observation of public access spaces with video surveillance devices shall be allowed for reasons of security, of heritage conservation, where there is a relevant interest, or where it is established by an ecclesiastical authority or a specifically applicable norm.

§ 2. The fact of the video surveillance, and the name of the data controller, must be identifiable by means of appropriate signs, except where such publicity impedes the legitimate objective pursued with the measure or involves a disproportionate effort.

§ 3. Storage or use of the data collected in accordance with § 1 of this Article is allowed, in so far as this is necessary for the achievement of the objective pursued, and provided there is no indication that the interests of the data subjects should prevail. If the data collected by video surveillance refers to a specific person, he/she must be notified in accordance with Articles 15 and 16.5. The data should be deleted immediately when it is no longer necessary to achieve the objective, or if the protected interests of the data subjects prevent further storage.

Article 44. Processing of data in the workplace

The personal data of an employee, including data on religious affiliation, religious beliefs and fiduciary duties, may be processed for employment purposes, for the performance of the employment contract. These may include compliance with legal obligations or obligations derived from the collective agreement, the management, planning and organization of work, equality and diversity in the workplace, health and safety at work, protection of the assets of employees or clients, as well as for the exercise and enjoyment, individually or collectively, of the rights and benefits related to employment, and effects of the termination of the employment relationship.

Article 45. Parochial Registers concerning the Sacraments

The Registers concerning the Sacraments are governed by the norms of Canon Law.

Article 46. Codes of conduct

§ 1. The Archbishop may approve models of Codes of Conduct to be applied in terms of data protection, which, without prejudice to other contents, shall contain the regulation of out-of-court procedures and other procedures for the resolution of conflicts, that allow to resolve the controversies related to the processing between controller and the data subjects.

§ 2. The Data Protection Officer shall promote the elaboration of codes of conduct according to the models mentioned in § 1 of this Article, which, in any case, shall be destined to contribute to the correct application of this General Decree.

§ 3. The codes of conduct referred to in § 2 of this Article, shall be approved, modified and suppressed by the competent ecclesiastical authorities, following a report from the

Data Protection Officer of the Archdiocese, and shall be mandatory for the controllers to whom they are addressed.

§ 4. Supervision of compliance with a code of conduct shall correspond to the competent Data Protection Officer.

§ 5. The draft code or its modification or extension may be presented, for the applicable purposes, and always through the Data Protection Officer of the Archdiocese of Malta, to the competent supervisory authority.

Article 47. Regulatory development

The Bishop and, where applicable, the different ecclesiastical authorities with canonical legislative power referred to in Article 3 of this General Decree, in relation to canons 131 and 135 §§ 1-2 CIC, may dictate further regulations, but are to ensure proper legal uniformity with this General Decree

Article 48. Entry into Force

This General Decree, shall enter into force on May 21, 2018 in accordance with Canons 455 § 4 and 8 § 2 CIC.

Index
Preamble
Chapter 1. General provisions

Article 1. Objective
Article 2. Scope of material application
Article 3. Scope of organizational application
Article 4. Definitions

Chapter II. Principles
Article 5. Secrecy of data
Article 6. Lawfulness of the processing of personal data
Article 7. Conditions for the processing of personal data
Article 8. Consent
Article 9. Communication between ecclesiastical entities or ecclesiastical authorities
Article 10. Disclosure to non-ecclesiastical or public authorities
Article 11. Processing of special categories of personal data
Article 12. Processing of personal data relating to convictions and criminal offenses
Article 13. Processing that does not require identification

Chapter III. Obligations of the controller's information and rights of the data subject

Section 1. Obligations of the controller's information
Article 14. Transparency of the information and procedures for exercising the rights of the data subject
Article 15. Information that should be provided when the data is obtained from the data subject
Article 16. Information to be provided when the personal data has not been obtained from the data subject

Section 2. Rights of the data subject
Article 17. Right of access of the data subject
Article 18. Right of rectification
Article 19. Right of withdrawal of consent
Article 20. Right to restriction of processing
Article 21. Obligation to notify regarding rectification or deletion of personal data or restriction of processing
Article 22. Right to data portability
Article 23. Right of object
Article 24. Individual automated decisions, including profiling
Article 25. Provisions common to the rights of the data subject

Chapter IV. Data Controllers and Processors

Section 1. Technology and organization; work processing
Article 26. Technical and organizational measures
Article 27. Design and default configurations
Article 28. Joint controllers
Article 29. Processors
Article 30. Processing under the authority of data controller or the processor