SUBSIDIARY LEGISLATION 586.08

DATA PROTECTION (PROCESSING OF PERSONAL DATA BY COMPETENT AUTHORITIES FOR THE PURPOSES OF THE PREVENTION, INVESTIGATION, DETECTION OR PROSECUTION OF CRIMINAL OFFENCES OR THE EXECUTION OF CRIMINAL PENALTIES) REGULATIONS

28th May, 2018*

LEGAL NOTICE 168 of 2018, as amended by Legal Notice 108 of 2020.

PART I
GENERAL PROVISIONS

Citation.

1. (1) The title of these regulations is the Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations.

(2) These regulations transpose Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

Interpretation.
Amended by:
L.N. 108 of 2020.

2. In these regulations, unless the context otherwise requires:

"Act" means the Data Protection Act; Cap. 586.

"adequacy decision" means a decision adopted by the European Commission pursuant to article 36(3) of the Directive mentioned in regulation 1(2), that a third country, a territory or one or more specified sectors within that third country, or an international organisation ensures an adequate level of protection;

"biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

"Commissioner" means the Information and Data Protection Commissioner established under article 11 of the Act; Cap. 586

*See Legal Notice 172 of 2018.

"competent authorities" means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and excluding the Security Service as established under the Security Service Act;

Cap. 391

(b) any other body or entity entrusted by law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

"controller" means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data;

"data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his health status;

"the Directive" means Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data;

"filing system" means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

"genetic data" means personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

"international organisation" means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries. For the purposes of these regulations, the International Criminal Police Organisation (‘Interpol’) shall be considered as an international organisation;

"personal data" means any information relating to an identified

or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, 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 natural person;

"personal data breach" means 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;

"processing" means any operation or set of operations which is performed on personal data or on 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;

"processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

"pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

"recipient" means a natural or legal person, public authority, agency or another body, to which personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

"restriction of processing" means the marking of stored personal

data with the aim of limiting their processing in the future;

"supervisory authority" means an independent public authority established in another Member State pursuant to article 41 of the Directive mentioned in regulation 1(2).

"union bodies" means agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the Treaty on the Functioning of the European Union, or any subsequent treaty and other agencies, offices and bodies established by Union law and authorised by law to process personal data for any of the purposes set out in regulation 3(1), where the law provides for the communication of such personal data by competent authorities to such agencies, offices and bodies;

"user" means a natural person authorised by the controller or the processor to access and use any automated processing system.

Applicability of these regulations.

3. (1) These regulations shall apply to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security:

Provided that the specific provisions for the protection of personal data in union legal acts adopted by the European Union that entered into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of the Directive, shall remain unaffected.

(2) These regulations shall apply to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

(3) These regulations shall not apply to the processing of personal data by competent authorities for a purpose other than the purposes set out in sub-regulation (1).

(4) These regulations shall not apply to the processing of personal data by competent authorities for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes unless such processing is performed for any of the purposes set out in sub-regulation (1).

PART II
PRINCIPLES

Principles relating to processing of personal data.

4. (1) Personal data shall be:

(a) processed lawfully and fairly;

(b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are processed;

(d) 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;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

(2) Processing by the same or another controller for any of the purposes set out in regulation 3(1) other than that for which the personal data are collected shall be permitted in so far as:

(a) the controller is authorised to process such personal data for such purpose in accordance with law; and

(b) processing is necessary and proportionate to that other purpose in accordance with law.

(3) Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in regulation 3(1), subject to appropriate safeguards for the rights and freedoms of data subjects.

(4) The controller shall be responsible for, and be able to demonstrate compliance with sub-regulations (1), (2) and (3).

Time-limits for storage and review.

5. (1) Personal data which is no longer required for the purposes set out in regulation 3(1) shall be erased without undue delay.

(2) Without prejudice to any time limits for storing or erasing data provided for by any law, the controller shall establish appropriate time limits for the erasure of personal data or for a periodic review of the need for the storage of personal data. The controller shall be responsible for establishing a data-retention policy, which shall include all the data categories and the respective time-limits.

(3) The data retention policy and any subsequent amendments thereto, shall be reviewed and approved by the Commissioner. The Commissioner may refuse a data retention policy if it does not comply with these regulations.

(4) The controller shall be responsible for establishing the necessary procedural measures, including, but not limited to, the necessary technical arrangements, in order to ensure that the obligations laid down in sub-regulation (2) are met.

Distinction between different categories of data subjects.

6. The controller, where applicable and as far as possible, shall make a clear distinction between personal data of different categories of data subjects, including:

(a) persons with regard to whom there are serious ground for believing that they have committed or are about to commit a criminal offence;

(b) persons convicted of a criminal offence;

(c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he could be the victim of a criminal offence; and

(d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in paragraphs (a) and (b).

Distinction between personal data and verification of quality of personal data.

7. (1) Personal data based on personal assessment shall be distinguished from personal data based on facts.

(2) The competent authorities shall take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available.

(3) The competent authorities shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. Where possible, in all transmission of personal data, the competent authorities shall ensure that:

(a) personal data based on opinions or personal assessments shall be checked at source prior to its transmission and its degree of reliability or accuracy shall be clearly indicated;

(b) personal data consisting of judicial decisions or decisions not to prosecute shall be clearly indicated as such; and

(c) necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date shall be added.

(4) The recipient shall be notified without delay if it emerges that incorrect personal data have been transmitted or that personal data have been unlawfully transmitted. In such a case, the personal data shall be rectified or erased or processing shall be restricted in accordance with regulation 16.

Lawfulness of processing.

8. (1) Processing shall be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in regulation 3(1) and that is based on law.

(2) The competent authorities in accordance with law shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.

(3) It shall be lawful for competent authorities to collect personal data by technical surveillance or other automated means for any of the purposes set out in regulation 3(1) and that is based on law.

Specific processing conditions.

9. (1) Personal data collected by competent authorities for the purposes set out in regulation 3(1) shall not be processed for purposes other than those set out in regulation 3(1) unless such processing is authorised by law and is carried out in accordance with the applicable data protection rules.

(2) Where a law provides specific conditions for processing, the transmitting competent authority shall inform the recipient of personal data of the conditions and the requirement to comply with them.

(3) The competent authority shall not apply the conditions referred to in sub-regulation (2) to recipients in other Member States or to Union Bodies, which differ from those applicable to similar transmissions of data between competent authorities within Malta.

Processing of special categories of personal data.

10. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic 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 shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only;

(a) where authorised by law;

(b) to protect the vital interests of the data subject or of another natural person; or

(c) where such processing relates to data which are manifestly made public by the data subject.

Automated individual decision-making.

11. (1) A decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him, shall be prohibited unless authorised by a law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

(2) Decisions referred to in sub-regulation (1) shall not be based on special categories of personal data referred to in regulation 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

(3) Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in regulation 10 shall be prohibited.

PART III
RIGHTS OF THE DATA SUBJECT

Communication and modalities for exercising the rights of the data subject.

12. (1) The controller shall take reasonable steps to provide any information referred to in regulation 13 and ensure that any communication with regard to regulations 11, 14 to 18 and 31 relating to the processing is provided in a concise, intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including by electronic means. As a general rule, the controller shall provide the information in the same form as the request.

(2) The controller shall facilitate the exercise of the rights of the data subject under regulations 11 and 14 to 18.

(3) The controller shall inform the data subject in writing about the follow up to his request without undue delay.

(4) The information provided under regulation 13 and any communication made or action taken pursuant to regulation 11, 14 to 18 and 31 are to be provided free of charge:

Provided that where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

(5) Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in regulations 14 or 16, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Information to be made available or given to the data subject.

13. (1) The controller shall make available to the data subject at least the following information:

(a) the identity and the contact details of the controller;

(b) the contact details of the Data Protection Officer, where applicable;

(c) the purposes of the processing for which the personal data are intended;

(d) the right to lodge a complaint with the Commissioner and the contact details of the Commissioner;

(e) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject.

(2) In addition to the information referred to in sub-regulation (1), the controller shall give to the data subject, in specific cases, the following further information to enable the exercise of his rights:

(a) the legal basis for the processing;

(b) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period;

(c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations;

(d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

(3) The information pursuant to sub-regulation (2) based on any other national law may be delayed, restricted or omitted, for as long as this constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

Right of access by the data subject.

14. Subject to the regulation 15, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of and legal basis for the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction

of processing of personal data concerning the data subject;

(f) the right to lodge a complaint with the Commissioner and the contact details of the Commissioner;

(g) communication of the personal data undergoing processing and of any available information as to their origin.

Limitations to the right of access.

15. (1) The data subject's right of access may be restricted, wholly or partly, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, for any of the reasons mentioned in regulation 13(3)(a) to (e).

(2) In the cases referred to in sub-regulation (1), the controller shall inform the data subject, without undue delay, and in no later than forty days from receiving the request, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction:

Provided that such information may be omitted where the provision thereof would undermine a purpose under sub-regulation (1).In any case, the controller shall inform the data subject of the possibility of lodging a complaint with the Commissioner or seeking a judicial remedy.

(3) The controller shall document the factual or legal reasons on which the decision under sub-regulation (1) and (2) is based and such information shall be made available to the Commissioner.

Right to rectification or erasure of personal data and restriction of processing.

16. (1) The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data relating to him. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

(2) The controller shall erase personal data without undue delay and provide for the right of the data subject to obtain from the controller the erasure of personal data concerning him without undue delay where processing infringes the provisions adopted pursuant to regulations 4, 8 or 10, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject.

(3) Instead of erasure, the controller shall restrict processing where:

(a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be

ascertained; or

(b) the personal data must be maintained for the purposes of evidence:

Provided that where processing is restricted pursuant to sub-regulation (3)(a), the controller shall inform the data subject before lifting the restriction of processing.

(4) Regulation 15 on the limitation to the right of access shall apply *mutatis mutandis* to the right to rectification or erasure of personal data and restriction of processing.

(5) The controller shall communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originate.

(6) Where personal data has been rectified or erased or processing has been restricted pursuant to sub-regulation (1), (2) and (3), the controller shall notify the recipients of such data and the recipients shall rectify or erase the personal data or restrict processing of the personal data under their responsibility.

Exercise of rights by the data subject and verification by the commissioner.

17. (1) In the cases referred to in regulation 13(3), regulation 15(2) and regulation 16(4), the data subject may also exercise his rights through the Commissioner.

(2) The controller shall inform the data subject of the possibility of exercising his rights through the Commissioner pursuant to sub-regulation (1).

(3) Where the right referred to in sub-regulation (1) is exercised, the Commissioner shall inform the data subject at least that all necessary verifications or a review by the Commissioner has taken place. The Commissioner shall also inform the data subject of his right to seek a judicial remedy.

Rights of the data subject in criminal investigations and proceedings.

18. Where a law provides in an equivalent manner for the rights referred to under regulations 13, 14 and 16 with regard to personal data contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings, the data subject shall exercise his rights in accordance with such other law.

PART IV
CONTROLLER AND PROCESSOR

Title I
General Obligations

Obligations of the controller.

19. (1) The controller, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with these regulations, including where proportionate, the implementation of appropriate data protection policies by the controller.

(2) The measures referred to in sub-regulation (1) shall be reviewed and updated where necessary.

Data protection by design and by default.

20. (1) The controller, 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, both at the time of the determination of the means for processing and at the time of the processing itself, shall implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing, in order to meet the requirements of these regulations and protect the rights of data subjects.

(2) The controller shall implement appropriate technical and organisational measures ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Joint controllers.

21. (1) Where two or more controllers jointly determine the purposes and means of processing, they shall be deemed to be joint controllers.

(2) Joint controllers shall, in a transparent manner, determine their respective responsibilities for compliance with these regulations, in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information referred to in regulation 13, by means of an arrangement between them unless, and

in so far as, the respective responsibilities of the controllers are determined by law.

(3) Joint controllers shall designate which controller of them is to act as a single contact point for data subjects:

Provided that where the single contact point is determined by a law, that law shall apply notwithstanding any agreement between the controllers.

Processor.

22. (1) Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of these regulations and ensure the protection of the rights of the data subject.

(2) It shall not be lawful for the processor to engage another processor without prior specific or general written authorisation by the controller:

Provided that in the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

(3) The processing by a processor shall be governed by a contract, 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 shall stipulate, in particular, that the processor:

(a) acts only on instructions from the controller;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;

(d) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless the storage of such personal data is required by law;

(e) makes available to the controller all information

necessary to demonstrate compliance with this regulation;

(f) complies with the conditions referred to in sub-regulations (2) and (3) for engaging another processor.

(g) assists the controller in ensuring compliance with the obligations pursuant to regulations 29 to 31 taking into account the nature of processing and the information available to the processor;

(4) The contract referred to in sub-regulation (3) shall be in writing, including in an electronic form.

(5) If a processor determines, in infringement of these regulations, the purposes and means of processing, that processor shall be considered to be a controller in respect of that processing.

Processing under the authority of the controller or processor.

23. The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by law.

Records of processing activities.

24. (1) Controllers shall maintain a record of all categories of processing activities under their responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller and the Data Protection Officer;

(b) the purposes of the processing;

(c) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(d) a description of the categories of data subjects and of the categories of personal data;

(e) where applicable, the use of profiling;

(f) where applicable, the categories of communications and of transfers of personal data in accordance with Part V of these regulations;

(g) where applicable, the details of the authority, body, agency, office or person making the request referred to in regulation 35(2);

(h) where applicable, the purpose and reason for the

request referred to in regulation 35(2) and, or, of communication or transfer of personal data, as the case may be;

(i) where applicable, the date of communication or transfer of personal data;

(j) an indication of the legal basis for the processing operations, including communications and transfers, for which the personal data are intended;

(k) where possible, the envisaged time limits for erasure of the different categories of personal data;

(l) where possible, a general description of the technical and organisational security measures referred to in regulation 29(1).

(2) Processors shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) t he name and contact details of the processor or processors, of each controller on behalf of which the processor is acting and, where applicable, the Data Protection Officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, communications and transfers of personal data where explicitly instructed to do so by the controller, including the identification of the recipient;

(d) where possible, a general description of the technical and organisational security measures referred to in regulation 29(1).

(3) The records referred to in sub-regulations (1) and (2) shall be in writing, including in electronic form.

(4) The controller and the processor shall make the records referred to in sub-regulations (1) and (2) available to the Commissioner on request.

Logging.

25. (1) Controllers, and where applicable processors, shall ensure that processing operations in automated processing systems relating to at least collection, alteration, consultation, disclosure including transfers, combination and erasure are logged.

(2) The logs referred to in sub-regulation (1) shall include at least the date and time of such operations and, as far as possible, the identification of the user performing such processing operation:

Provided that the logs of consultation and disclosure shall also include the justification for such operations, and as far as possible, the identity of the recipients of such personal data other than the user.

(3) The logs shall be only used for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.

(4) The controller and the processor shall make the logs available to the Commissioner upon request.

Cooperation with the Commissioner.

26. The controller and the processor shall cooperate with the Commissioner in the performance of his tasks in accordance with regulation 48 upon request.

Data protection impact assessment.

27. (1) Where a type of processing, in particular, using new technologies, and taking into 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 carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) The assessment referred to in sub-regulation (1) shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with these regulations, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

Prior consultation with the Commissioner.

28. (1) The controller or the processor shall consult with the Commissioner prior to processing of personal data which will form part of a new filing system to be created, where:

(a) a data protection impact assessment as provided for in regulation 27 indicates that the processing would result in a high risk, in the absence of measures taken by the controller to mitigate the risk; or

(b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

(2) The Commissioner shall be consulted during the preparation of a proposal for a legislative measure to be adopted by Parliament or of a regulatory measure based on such a legislative measure, which relates to processing.

(3) The Commissioner may establish a list of the processing operations which are subject to prior consultation pursuant to sub-regulation (1).

(4) The controller shall provide the Commissioner with the data protection impact assessment pursuant to regulation 27 and, on request, with any other information to allow the Commissioner to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

(5) Where the Commissioner is of the opinion that the intended processing referred to in sub-regulation (1) would infringe any regulation under these regulations, in particular where the controller has insufficiently identified or mitigated the risk, the Commissioner shall, within six weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable, to the processor, and may use any of its powers referred to in regulation 49:

Provided that such period may be extended by a month, taking into account the complexity of the intended processing.

(6) The Commissioner shall inform the controller and, where applicable, the processor of any extension as provided for in the proviso of sub-regulation (5) within one month of receipt of the request for consultation, together with the reasons for the delay.

Title II
Security of Personal Data

Security of processing.

29. (1) The controller and the processor shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular in relation to the processing of special categories of personal data referred to in regulation 10.

(2) In respect of automated processing, the controller or the processor shall, following an evaluation of the risks, implement measures designed to:

(a) deny unauthorised persons access to processing equipment used for processing ('equipment access control');

(b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control');

(c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control');

(d) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control');

(e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control');

(f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control');

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');

(i) ensure that installed systems may, in the case of interruption, be restored ('recovery');

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunction of the system ('integrity').

Notification of a personal data breach to the Commissioner.

30. (1) In the case of a personal data breach, the controller shall notify in writing, including in an electronic form, without undue delay and, where feasible, not later than seventy two hours after having become aware of it, the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons:

Provided that where the notification to the Commissioner is not made within seventy two hours, it shall be accompanied by reasons for the delay.

(2) The processor shall notify in writing, including in an electronic form, the controller without undue delay after becoming aware of a personal data breach:

Provided that where, taking into account the severity of the personal data breach and the possible consequences that may ensue if the controller is not notified immediately, the processor may notify the controller through other means. In such case, the notification in writing, including in an electronic form, shall be made nonetheless.

(3) The notification referred to in sub-regulation (1) shall at least:

(a) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(4) Where, and in so far as, it is not possible to provide the information mentioned under sub-regulation (3) at the same time, the information may be provided in phases without undue delay.

(5) The controller shall document any personal data breaches referred to in sub-regulation (1), comprising the facts relating to the personal data breach, its effects and the remedial action taken in a way as to enable the Commissioner to verify compliance with this regulation.

(6) Where the personal data breach involves personal data that have been transmitted by or to the controller of another Member State, the information referred to in sub-regulation (3), shall be communicated to such controller without undue delay.

Communication of a personal data breach to the data subject.

31. (1) In the case of a personal data breach which is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach, in writing, to the data subject without undue delay:

Provided that in cases where it is not feasible to communicate the data breach to the data subject in writing, or where due to the severity of the personal data breach and the possible

consequences that may ensue if the communication of a personal data breach to the data subject is not made immediately, such communication may be made through other means.

(2) The communication to the data subject referred to in sub-regulation (1) shall describe in clear and plain language the nature of the personal data breach and shall contain at least the information and measures referred to in regulation 30(3)(b), (c) and (d).

(3) The communication to the data subject referred to in sub-regulation (1) shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technological and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in sub-regulation (1) is no longer likely to materialise;

(c) it would involve a disproportionate effort:

Provided that in such a case, there shall be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.

(4) If the controller has not already communicated the personal data breach to the data subject, the Commissioner, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so, or may decide that any of the conditions referred to in sub-regulation (3) are met.

(5) The communication to the data subject referred to in sub-regulation (1) may be delayed, restricted or omitted subject to the conditions and on the grounds referred to in regulation 13(3).

(6) A record shall be kept of the date, time, and means of the communication to the data referred to in sub-regulation (1), and where applicable, the reason for making such communication to the data subject through other means pursuant to the proviso to the same sub-regulation.

(7) Where the controller decides that a communication to the data subject referred to in sub-regulation (1), is not required for any of the reasons mentioned in sub-regulation 3(a) to (c), the controller shall

document the reasons for such decision.

(8) Where the communication to the data subject referred to in sub-regulation (1) has been delayed, restricted or omitted in accordance with sub-regulation (5), the controller shall document the reasons for such delay, restriction or omission.

Title III
Data Protection Officer

Designation of the Data Protection Officer.

32. (1) The controller shall designate a Data Protection Officer.

(2) The obligation under sub-regulation (1) shall not apply to courts and tribunals any other independent judicial authorities when acting in their judicial capacity.

(3) The Data Protection Officer shall be designated on the basis of his professional qualities and, in particular, his expert knowledge of data protection law and practice and ability to fulfil the tasks referred to in regulation 34.

(4) A single Data Protection Officer may be designated for several competent authorities, taking account of their organisational structure and size.

(5) The controller shall publish the contact details of the Data Protection Officer and communicate them to the Commissioner.

Position of the Data Protection Officer.

33. (1) The controller shall ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(2) The controller shall support the Data Protection Officer in performing the tasks referred to in regulation 34 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his expert knowledge.

(3) The controller shall ensure that the Data Protection Officer does not receive any instructions regarding the exercise of the tasks referred to in regulation 34:

Provided that the Data Protection Officer shall report directly to the highest level of management.

(4) The Data Protection Officer shall not be dismissed or penalised by the controller for performing the tasks referred to in regulation 34.

Tasks of the Data Protection Officer.

34. The controller shall entrust the Data Protection Officer at least with the following tasks:

(a) to inform and advise the controller and the employees who carry out processing operations of their obligations pursuant to these regulations and other data protection legal provisions;

(b) to monitor compliance with these regulations, with other data protection legal provisions and with the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested in relation to the data protection impact assessment and monitor its performance pursuant to regulation 27;

(d) to cooperate with the Commissioner; and

(e) to act as the contact point for the Commissioner on issues relating to processing, including the prior consultation referred to in regulation 28, and to consult, where appropriate, with regard to any other matter.

PART V
COMMUNICATION AND TRANSFERS OF PERSONAL DATA

Title I
General Conditions for communication and transfers of personal data

Of the modalities of the requests for communication and transfers of personal data.

35. (1) A communication or transfer of personal data by a competent authority shall only take place upon request in writing, unless any other law or any international agreement to which Malta is a party provides otherwise.

(2) The request referred to in sub-regulation (1) shall include an indication of person or body making the request and the reason and purpose for which the request is made, unless any other law or any international agreement to which Malta is a party provides otherwise.

(3) The competent authority receiving a request as referred to in sub-regulation (1) shall reply in writing informing the person or body making the request of the decision taken as to whether the request can be met or not.

(4) Notwithstanding the requirements mentioned in sub-regulation (1), a competent authority may, without any prior request

being necessary, communicate or transfer personal data to:

(a) competent authorities in other Member States or to union bodies, in cases where there are factual reasons to believe that the data could assist in the detection, prevention, investigation or prosecution of any serious criminal offences or terrorist offences;

(b) any other recipient where the transfer of such personal data arises out of the necessity of the communicating or transferring competent authority in the execution of its duties for the purposes set out in regulation 3(1).

Communication or transfer of personal data transmitted or made available by another Member State.

36. (1) Where personal data are transmitted or made available by another Member State, such data may be communicated or transferred only if that Member State has given its prior authorisation to the communication or transfer.

(2) Communications or transfers without the prior authorisation of another Member State in accordance with sub-regulation (1) may be permitted only if the communication or transfer of the personal data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time:

Provided that the authority responsible for giving prior authorisation shall be informed without delay.

(3) Sub-regulation (1) shall not apply in cases where the communication of personal data takes place in the performance of a legal task by the competent authority making such communication in relation to the particular case for which the data was specifically transmitted or made available.

Title II
Communication of Personal Data Locally and within the European Union

Communication of personal data to other competent authorities.

37. (1) A communication of personal data, to other competent authorities, shall take place, if the transfer is necessary:

(a) for the purposes set out in regulation 3(1);

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

(c) to safeguard the legitimate interests of the data subject or the controller:

Provided that the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned do not override the interests necessitating the communication.

(2) A communication of personal data as contemplated in sub-regulation (1) may also take place if:

(a) there exists a legal obligation or authorisation to communicate such personal data; or

(b) the Commissioner authorises such communication of personal data.

Communication of personal data to government departments, public bodies and entities established by law, and to private parties. *Amended: L.N. 108 of 2020.*

38. (1) A communication of personal data to government departments or other public entities or bodies established by law, or to other private parties may only take place, if:

(a) the communication is strictly necessary for the performance of a task of the transferring competent authority as provided for by law for the purposes set out in regulation 3(1);

(b) the communication is strictly necessary in order to protect the vital interests of the data subject or another person;

(c) in an individual case for the establishment, exercise or defence of legal claims relating to the purposes set out in regulation 3(1) or resulting from, or otherwise relating to, a criminal offence:

Provided that the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned do not override the interests necessitating the communication:

Provided further that the data communicated to private parties shall be limited to what is strictly necessary to adequately identify the persons mentioned under regulation 6(a) in order to exercise his rights under this paragraph.

(d) there exists a legal obligation or authorisation to communicate such personal data; or

(e) the Commissioner authorises such communication of personal data.

(2) In exceptional circumstances, a communication of personal data to government departments or other public entities or bodies established by law, or to other private parties may take place, if:

(a) it is clearly in the interest of the data subject and the data subject himself has consented to the communication; or

(b) it is strictly necessary for the prevention of a serious and imminent danger.

Communication of personal data to authorities in other Member States competent for the purposes set out in sub-regulation 3(1) and to Union bodies.

39. Without prejudice to the provisions of any law or regulation laying down specific rules on the processing or exchange of personal data in the context of police and judicial cooperation, a communication of personal data to authorities in other Member States competent for the purposes set out in regulation 3(1) or to Union bodies may only take place, if:

(a) there exists a legal obligation or authorisation under any law or an international obligation under a treaty, convention or international agreement on mutual assistance, to which Malta is a party;

(b) the communication is strictly necessary for the prevention of a serious and imminent danger; or

(c) the communication is strictly necessary for the suppression of a serious criminal offence or a terrorist offence.

Processing of communicated personal data.

40. (1) Personal data communicated by a competent authority to other government departments or to bodies established by law, or to other private parties, shall not be used for purposes other than those specified in the request for communication of personal data without the authorisation of the competent authority from which such personal data was made available or obtained.

(2) Where the recipient of personal data referred to in sub-regulation (1) requires such data for purposes other than those for which it was requested, the recipient shall submit a new request to the competent authority in accordance with regulation 35(1), and that data shall not be used by the recipient for purposes other than those included in the original request unless there is written authorisation.

Title III
Transfers of Personal Data to Third Countries or International Organisations

General principles for transfers of personal data.

41. (1) Any transfer by competent authorities of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation including for onward transfers to another third country or international organisation shall take place, subject to compliance with these regulations, only where the conditions laid down in this Part are met, namely:

(a) the transfer is necessary for the purposes set out in regulation 3(1);

(b) the personal data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in regulation 3(1);

(c) an adequacy decision has been adopted:

Provided that in the absence of such decision, such transfers of personal data may take place where appropriate safeguards have been provided or exist pursuant to regulation 43:

Provided further that in the absence of an adequacy decision, and of appropriate safeguards in accordance with regulation 43, such transfers may take place where derogations for specific situations apply pursuant to regulation 44.

(d) in the case of an onward transfer to another third country or international organisation, the competent authority that carried out the original transfer or another competent authority of the same Member State authorises the onward transfer, after taking into due account all relevant factors, including:

(i) the seriousness of the criminal offence;

(ii) the purpose for which the personal data was originally transferred; and

(iii) the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

Transfers on the basis of an adequacy decision.

42. (1) Where an adequacy decision has been adopted, a transfer of personal data to the third country, a territory or one or more specified sectors within that third country, or an international organisation, in relation of which such adequacy decision has been adopted, may take place without requiring any specific authorisation.

(2) The repealing, amendment, or suspension of an adequacy decision shall be without prejudice to transfers of personal data to the third country, the territory or one or more specified sectors within that third country, or the international organisation with regards to transfers pursuant to regulations 43 and 44.

Transfers subject to appropriate safeguards.

43. (1) In the absence of an adequacy decision, a transfer of personal data to a third country or an international organisation may take place where:

(a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or

(b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data.

(2) The controller shall inform the Commissioner about categories of transfers under sub-regulation (1)(b).

(3) When a transfer is based on sub-regulation (1)(b), such a transfer shall be documented.

(4) The documentation referred to in sub-regulation (3) shall at least include:

(a) the date and time of the transfer;

(b) information about the recipient;

(c) the justification for the transfer; and

(d) the personal data transferred.

(5) The documentation referred to in sub-regulation (3) shall be made available to the Commissioner on request.

Derogations for specific situations.

44. (1) In the absence of an adequacy decision, or of appropriate safeguards pursuant to regulation 43, a transfer or a category of transfers of personal data to a third country or an international organisation may take place only on the conditions that the transfer is necessary:

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

(b) to safeguard legitimate interests of the data subject, where the law so provides;

(c) for the prevention of an immediate and serious threat to public security of a Member State or a third country;

(d) in individual cases for the purposes set out in regulation 3(1); or

(e) in an individual case for the establishment, exercise or defence of legal claims relating to the purposes set out in regulation 3(1).

(2) Personal data shall not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in a transfer set out in sub-regulation (1)(d) and (e).

(3) The provisions of regulation 43(3) to (5), on the transfers subject to appropriate safeguards, shall apply *mutatis mutandis* to transfers pursuant to sub-regulation (1).

Transfers of personal data to recipients established in third countries.

45. (1) By way of derogation from regulation 41(1)(b) and without prejudice to any international agreement referred to in sub-regulation (2), competent authorities, in individual and specific cases, may transfer personal data directly to recipients established in third countries only if the other provisions of these regulations are complied with and all of the following conditions are fulfilled:

(a) the transferring competent authority is a public authority;

(b) the transfer is strictly necessary for the performance of a task of the transferring competent authority as provided for by law for the purposes set out in regulation 3(1);

(c) the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand;

(d) the transferring competent authority considers that the transfer to an authority that is competent for the purposes referred to in regulation 3(1) in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;

(e) the authority that is competent for the purposes referred to in regulation 3(1) in the third country is informed without undue delay, unless this is ineffective or inappropriate;

(f) the transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the recipient provided that such processing is necessary.

(2) An international agreement referred to in sub-regulation (1) shall be any bilateral or multilateral international agreement in force between Malta and third countries in the field of judicial cooperation in criminal matters and police cooperation.

(3) The transferring competent authority shall inform the Commissioner about transfers under this regulation.

(4) The provisions of regulation 43 (3) to (5) on the transfers subject to appropriate safeguards, shall apply *mutatis mutandis* to transfers pursuant to sub-regulation (1).

Relationship with previously concluded international agreements in the field of judicial cooperation in criminal matters and police cooperation.

46. Any international or bilateral agreement involving the transfer of personal data to third countries or international organisations which were concluded by Malta prior to 6 May 2016 and which comply with applicable Union law shall remain in force until amended, replaced, or revoked.

PART VI
THE COMMISSIONER

Limitations on the competency of the Commissioner.

47. The Commissioner shall not be competent for the supervision of processing operations of courts and tribunals when acting in their judicial capacity.

Tasks of the Commissioner.

48. (1) The tasks of the Commissioner are to:

(a) monitor and enforce the application of these regulations and the Implementing Acts adopted pursuant the Directive;

(b) promote the awareness of controllers and processors of their obligations under these regulations;

(c) upon request, provide information to any data subject concerning the exercise of their rights under these regulations or the Directive and, if appropriate, cooperate with supervisory authorities to that end;

(d) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with regulation 55, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with other supervisory authorities is necessary;

(e) check the lawfulness of processing pursuant to regulation 17, and inform the data subject within a reasonable period of the outcome of the check pursuant to regulation 17(3) or of the reasons why the check has not been carried out;

(f) cooperate with, including sharing information, and provide mutual assistance to supervisory authorities, with a view to ensuring the consistency of application and enforcement of the Directive;

(g) conduct investigations on the application of these

regulations, including on the basis of information received from a supervisory authority or other public authority;

(h) provide advice on the processing operations referred to in regulation 28;

(i) contribute to the activities of the European Data Protection Board;

(j) monitor relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communications technologies;

(k) keep internal records of infringements of these regulations and of measures taken;

(l) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;

(m) advise, in accordance with national law, the Parliament, the Government and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(n) perform any other task implied under any provision of these regulations.

(2) The Commissioner shall facilitate the submission of complaints referred to in sub-regulation 1(d) by measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(3) The performance of the tasks of the Commissioner shall be free of charge for the data subject and for the Data Protection Officer:

Provided that where a request by a data subject is manifestly unfounded or excessive, in particular because of its repetitive character, the Commissioner may charge a reasonable fee based on its administrative costs, or may refuse to act on the request.

(4) Where a fee is charged by the Commissioner pursuant to the proviso to sub-regulation (3), the Commissioner shall bear the burden of demonstrating that the request is manifestly unfounded or excessive.

49. The Commissioner shall have the following powers: Powers of the Commissioner.

(a) investigative powers consisting of the following:

(i) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information he requires for the performance of his tasks;

(ii) to carry out investigations including in the form of data protection audits;

(iii) to notify the controller or the processor of an alleged infringement of these regulations;

(iv) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks.

(b) corrective powers consisting of the following:

(i) to issue warnings to a controller or processor that intended processing operations are likely to infringe the provisions of these regulations;

(ii) to issue reprimands to a controller or a processor where processing operations have infringed any provision of these regulations;

(iii) to order the controller or the processor to comply with the data subject's requests to exercise his rights pursuant to these regulations;

(iv) to order the controller or processor to bring processing operations into compliance with the provisions of these regulations, where appropriate, in a specified manner and within a specified period;

(v) to order the controller to communicate a personal data breach referred to in regulation 31, to the data subject;

(vi) to impose a temporary or definitive limitation including a ban on processing;

(vii) to order the rectification or erasure of personal data or restriction of processing pursuant to regulation 16 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to regulation 16(6);

(viii) to impose an administrative fine pursuant to

regulation 57;

(ix) to order the suspension of data flows to a recipient in a third country or to an international organisation.

(c) authorisation and advisory powers consisting of the powers:

(i) to advise the controller in accordance with the prior consultation procedure referred to in regulation 28;

(ii) to issue, on its own initiative or on request, opinions to Parliament, the Government or, in accordance with law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(iii) to approve data retention policies referred to in regulation 5(3); and

(iv) to authorise the communication of personal data where the law so requires.

Complaints by employees of the competent authority.

50. (1) Where an employee of the competent authority becomes aware that any of the provisions of these regulations have been, are being, or are about to be infringed in any way whatsoever, such employee shall be able to report such infringement directly to the Data Protection Officer of that competent authority.

(2) Where a report is made under sub-regulation (1), unless otherwise directed by the reporting employee himself, the Data Protection Officer shall take every reasonable step to ensure that the identity of such employee is not disclosed or be discovered in any way.

(3) The provisions of sub-regulations (1) and (2) shall apply *mutatis mutandis* where such complaint is lodged with the Commissioner.

Commissioner's activity reports.

51. The Commissioner shall draw up an annual report on its activities, which shall include a list of types of infringement notified and fines imposed. This report shall be transmitted to Parliament, the Government and other authorities as designated by law, and it shall be available to the public.

Cooperation with supervisory authorities.

52. (1) Where in the application of the provisions of these regulations or the Directive aimed at protecting the rights of individuals with regard to the processing of personal data concerning them, the Commissioner requires information, assistance or the action

of a supervisory authority, the Commissioner may request such information, assistance or action to such supervisory authority.

(2) The request referred to in sub-regulation (1) shall contain all the necessary information, including the purpose of and reasons for the request. The information exchanged shall be used only for the purpose for which it was requested.

(3) Where the Commissioner receives a request for information, assistance, or for the exercise of any of its supervisory functions, or complaint, from a supervisory authority, the Commissioner shall in full spirit of cooperation, provide such information or assistance, or exercise its such supervisory function, or act upon such complaint as if such request or complaint has been received directly from a data subject.

(4) The Commissioner shall take all appropriate measures required to reply to a request referred to in sub-regulation (3), such as the transmission of relevant information on the conduct of an investigation, without undue delay and no later than one month after receiving the request.

(5) The Commissioner shall not refuse to comply with a request referred to in sub-regulation (3) unless:

(a) he is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b) compliance with the request would result in infringement of law.

(6) Where a request referred to in sub-regulation (3) is received, the Commissioner shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request:

Provided that where the Commissioner refuses to comply with such request pursuant to sub-regulation (5), he shall provide reasons for the refusal.

(7) Any communication transferred within the scope of this regulation, shall, as a rule, be made or supplied by electronic means, using the standardised format.

(8) The information received pursuant to this regulation shall be used only for the purpose for which it was requested.

(9) The Commissioner shall not charge a fee for complying and acting upon a request or complaint referred to under sub-regulation

(3), unless rules have been agreed between the Commissioner and the requesting supervisory authority for indemnification for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

PART VII
REMEDIES, LIABILITY AND FINES

Right to lodge a complaint with the Commissioner.

53. (1) Without prejudice to any administrative or judicial remedy, every data subject shall have the right to lodge a complaint with the Commissioner, if the data subject considers that the processing of personal data relating to him infringes these regulations.

(2) Where a complaint is lodged with the Commissioner by a data subject alleging that the processing of personal data relating to him in another Member State infringes the provisions of the Directive, the Commissioner shall transmit such complaint, without undue delay to the supervisory authority of that Member State, and the data subject shall be informed about the transmission.

(3) The Commissioner, following a complaint, shall provide further assistance to the data subject upon request.

(4) The Commissioner shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to regulation 54.

Right to an effective judicial remedy against the Commissioner. *Amended by: L.N. 108 of 2020.*

54. Article 31 of the Act shall apply *mutatis mutandis* where the Commissioner does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to regulation 53.

Representation of data subjects.

55. The data subject shall have the right to mandate a non-profit body, organisation or association which has been properly constituted in accordance with law, has statutory objectives which are in the public interest and is active in the field of data subject's rights and freedoms with regard to the protection of their personal data to lodge the complaint on his behalf.

General conditions for administrative fines.

56. (1) The Commissioner shall ensure that the imposition of administrative fines pursuant to regulation 57 are effective, proportionate and dissuasive.

(2) Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in regulation 49(1)(b).

(3) When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to regulation 20 and 29;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the Commissioner, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the Commissioner, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in regulation 49(1)(b) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; and

(j) any other aggravating or mitigating factor applicable to the circumstances of the case.

(4) If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of these regulations, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

Administrative fines.

57. The Commissioner may impose an administrative fine of not less than five hundred euro (€500) and not more than fifty thousand euro (€50,000), pursuant to regulation 56, for violating any of the following:

(a) the obligations of the controller and the processor

pursuant to regulation 19 to 34;

(b) the obligation to produce a data retention policy and any subsequent amendments pursuant to regulation 5;

(c) the basic principles for processing, pursuant to regulation 4, 8 and 10;

(d) the data subjects' rights pursuant to regulation 12 to 18;

(e) the transfers of communication and transfers of personal data pursuant to regulation 35 to 46:

Provided that the Commissioner may impose a daily fine of not more than fifty euro (€50) until the breach is rectified.