Depositor and Investor Compensation Schemes

GENERAL DATA PROTECTION REGULATION (GDPR)

Regulation 2016/679

FOR THE DEPOSITOR AND INVESTOR COMPENSATION SCHEME

Contents

Introduction 3
Definitions 4
Section 1 – Article 3 – Territorial Scope 5
Section 2: Article 5 – Principles relating to processing of personal data 5
Section 3: Article 6 – Lawfulness of processing 6
Section 4: Article 7 – Conditions for consent 7
Section 5: Article 9 – Processing of special categories of personal data 8
Section 6: Article 10 – Processing of personal data relating to criminal convictions and offences 10
Section 7 – Article 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject 10
Section 8: Article 15- Right of access by the data subject 11
Section 9: Article 16 – Right to rectification 12
Section 10 – Article 20- Right to data portability 14
Section 11- Article 21- Right to object 14
Article 22- Automated individual decision-making, including profiling 15
Section 11- Article 25 – Data Protection by design and by default 15
Section 12: Article 28 – Processor 16
Section 13: Article 30 – Records of processing activities 18
Section 14 Article 32 – Security of processing 19
Section 15- Article 33- Notification of a personal data breach to the supervisory authority 20
Section 16- Article 37 Designation of the data protection officer 20

Introduction

Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data known as the General Data Protection Regulation (GDPR) has become directly applicable in all Member States, including Malta as of the **25 May 2018**. This new Regulation will replace the EU's Data Protection Directive 95/46/EC which is currently transposed under the Data Protection Act (Chapter 440 of the Laws of Malta).

The GDPR retains the core rules stipulated by pervious data protection legislation and continues to regulate the processing of personal data with its goal being the protection of individuals.

This document has been developed to facilitate the depositor/investor in understanding their rights towards the Scheme's collection of data.

The GDPR Regulation will mainly affect the operations of the Depositor Compensation Scheme, and not that of the Investor Compensation Scheme since the DCS collects data of depositors, known as the Single Customer View data. In this document, the Scheme, will be explaining which articles mainly effect the Scheme and how the Scheme took all the necessary measures, to protect the data of depositors.

Definitions

'DCS' – *means The Depositor Compensation Scheme*

'DEPS'- *means Data Exchange and Payment Solution*

'DPO' – *means Data Protection Officer*

'EU' or 'Union'- *means European Union*

'GDPR' or 'Regulation' – *means General Data Protection Regulation 2016/679*

'ICS' – *means The Investor Compensation Scheme*

'SCV' – *means Single Customer View*

Section 1 – Article 3 – Territorial Scope

The Regulation primarily applies to the processing of personal data in the context of the activities of an establishment of a data controller or processor established within the European Union (EU), regardless of whether the processing itself takes place within the Union.

The Regulation however also applies to businesses based outside the Union that offer goods and services to, or monitor, individuals in the Union. Therefore, controllers and processors will be subject to the GDPR where the processing activities relate to:

- The offering of goods or services to individuals in the Union. It captures both free and paid for goods and services; and
- Monitoring the behaviour of individuals in the Union.

In the case of the above-mentioned businesses these are required to appoint a representative in the Union, subject to certain limited exemptions. The representative should be explicitly designated by means of a written mandate of the controller or processor to act on its behalf and should be subject to enforcement proceedings in the event of non- compliance by the controller or processor.

The DCS Regulations, transpose Directive 49/2014/EC on Deposit Guarantee Schemes, and therefore it operates in within the Union. The Scheme excludes participation by third country banks and therefore no depositor personal data will be transferred outside the Union.

Section 2: Article 5 – Principles relating to processing of personal data

Article 5 of the GDPR requires a controller[1] to ensure that:

A) Personal data is processed fairly, lawfully and in a transparent manner;
B) Personal data is only collected for specific, explicitly stated and legitimate purposes and is not processed for any purpose that is incompatible with that for which the information is collected;
C) Personal data that is processed is adequate, relevant and limited to what is necessary in relation to the purposes of the processing;
D) Personal data that is processed is accurate and, where necessary, up to date. All reasonable measures are taken to complete, correct, block or erase data to the extent that such data is incomplete or incorrect, having regard to the purposes for which that data is processed;

[1] The person who determines the purposes and means of processing of personal data

E) Personal data is kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data is processed;
F) Personal data is processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures.

The GDPR Regulations require that data is processed following the above mentioned requirements. The Scheme is in the process of having its own DEPS system in which the Scheme ensures that Depositors data is protected, processed lawfully, and ensures security of data transfer.

Section 3: Article 6 – Lawfulness of processing

The processing of the data must also satisfy at least one of the legal criteria under Article 6 of the GDPR. In the case where special categories of personal data are processed at least one of the legal criteria under Article 9[2] must also be satisfied.

Article 6:

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

a. the data subject has given consent to the processing of his/her personal data for one or more specific purposes;

b. processing is necessary[3] for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c. processing is necessary for compliance with **a legal obligation** to which the controller is subject;

The DCS, through this sub-article has satisfied the criteria to request personal data information, as per regulation 20 of the DCS Regulations.

d. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

e. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the

[3] Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

interests or fundamental rights and freedoms of the data subject which require protection of personal data, where the data subject is a child[4].

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

   a. Union law; or

   b. Member State law to which the controller is subject.

4. Where the processing for a purpose other than that for which the personal data has been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1)[5], the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data is initially collected, take into account, inter alia:

   a. any link between the purposes for which the personal data has been collected and the purposes of the intended further processing;

   b. the context in which the personal data has been collected, in particular regarding the relationship between data subjects and the controller;

   c. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9[6], or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10[7];

   d. the possible consequences of the intended further processing for data subjects;

   e. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Under the GDPR it is important to clearly understand and identify the legal ground for the processing of personal data.

Section 4: Article 7 – Conditions for 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.

[5] Of the GDPR
[6] Of the GDPR
[7] Of the GDPR

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. [2]Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his/her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. 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.

The Depositor Compensation Scheme does not rely on consent to obtain the data on depositors, as this requirement originates from a legal obligation.

Section 5: Article 9 – Processing of special categories of personal data

1. 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 prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

   a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

   b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

   c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

   d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to

persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside that body without the consent of the data subjects;

e) processing relates to personal data which is manifestly made public by the data subject;

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)[8] based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when that data is processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Special Categories of personal data

The Scheme may process categories of personal data in relation to employees. Such data is usually obtained from the employees themselves. When the processing for special categories of data is necessary for the Scheme to carry out its obligations and exercise specific rights in the field of employment and social security and social protection law in so far as it is authorized by law, the employees' explicit consent is not required for the processing of such data. Strict levels and access of rights apply in relation to special categories of personal data, hence allowing access only to those officials who must process the data in the course of their duties.

Section 6: Article 10 – Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1)[9] shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Regulation 14(3) of the DCS Regulations state that, the Scheme may suspend any payment referring to any account in respect of which a depositor or any person entitled to or interested in sums held therein has been charged with an offence arising out of or in relation to money laundering, pending the judgment of the court.

The Scheme will receive the data from the respective bank, which data is in turn received from the Courts of Law. The Scheme will keep such data and defer the payment of compensation accordingly.

Section 7 – Article 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject

Article 13- Information to be provided where personal data is collected from the data subject

Article 14- Information to be provided where personal data has not been obtained from the data subject.

The Regulation makes provision for the information which must be provided in privacy notices. It also requires controllers to ensure their privacy notices are 'Concise, transparent, intelligible and easily accessible'.

Section 8: Article 15- Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her is being processed, and, where that is the case, access to the personal data and the following information:

    a. the purposes of the processing;

    b. the categories of personal data concerned;

    c. the recipients or categories of recipient to whom the personal data has been or will be 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 or to object to such processing;

    f. the right to lodge a complaint with a supervisory authority;

    g. where the personal data is not collected from the data subject, any available information as to their source;

    h. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4)[10] and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data is transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46[11] relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

The Scheme is required that upon the request of the data subject to provide hhim/her with a confirmation as to whether or not personal data concerning him/her is being processed and if that is the case, allow access of such personal data and a copy of the data undergoing process.

Section 9: Article 16 – Right to rectification

Data subject may request controllers to rectify personal data that has not been processed in accordance with the GDPR, in particular because of the incomplete or inaccurate nature of the data. The controller shall immediately rectify or complete the data accordingly and notify any third parties to whom data had been disclosed about the measures undertaken.

Article 17- Right to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him/her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
    1. the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed;
    2. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1)[12], or point (a) of Article 9(2)[13], and where there is no other legal ground for the processing;
    3. the data subject objects to the processing pursuant to Article 21(1)[14] and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2)[15];
    4. the personal data has been unlawfully processed;
    5. the personal data has to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
    6. the personal data has been collected in relation to the offer of information society services referred to in Article 8(1)[16].
2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available

[12] Of the GDPR

technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers who are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, that personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

    1. for exercising the right of freedom of expression and information;

    2. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

    3. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2)[17] as well as Article 9(3)[18];

    4. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)[19] in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

    5. for the establishment, exercise or defence of legal claims.

Article 18- Right to restriction of processing

1. The data subject shall have the right to obtain from the controller, restriction of processing where one of the following applies:

    1. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

    2. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of its use instead;

    3. the controller no longer needs the personal data for the purposes of the processing, but it is required by the data subject for the establishment, exercise or defence of legal claims;

    4. the data subject has objected to processing pursuant to Article 21(1)[20] pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal 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

another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Section 10 – Article 20- Right to data portability

Data portability gives a further right to the data subject to get that personal data in a structured, commonly used and machine readable format. The data subject can also ask for the data to be transferred directly from one controller to another, where technically feasible. There is no right to charge fees for this service.

Provided that this applies:

1. only where the controller is processing personal data in reliance on the processing conditions of consent or performance of a contract.
2. only if the data processing is carried out by automated means and therefore does not cover paper files.
3. only to personal data concerning data subject.
4. only to personal data which is provided to the controller.

Section 11- Article 21- Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1)[21], including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data is 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. Where the data subject objects to processing for direct marketing purposes, the 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 paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

[21] Of the GDPR

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data is processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1)[22], the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him/her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22- Automated individual decision-making, including profiling

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

2. Paragraph 1 shall not apply if the decision:

    1. is necessary for entering into, or performance of, a contract between the data subject and a data controller;

    2. is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

    3. is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(2)1)[23], unless point (a) or (g) of Article 9(2)[24] applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 11- Article 25 – Data Protection by design and by default

The Regulation makes specific provisions on the use of technical and organisational measures tailored to enhance the level of data protection compliance. When deploying systems, applications, products or services that rely on the processing of personal data to fulfil their tasks, banks should take into account the right to data protection and should encourage their IT department or IT service providers, including developers, to design products or services that contain technical measures which are data protection friendly, embedded in the design.

[22] Of the GDPR
[23] Of the GDPR
[24] Of the GDPR

The DEPS is being designed, to protect depositor's data, through encryption.

Section 12: Article 28 – Processor

The GDPR impacts on all aspects of the processing relationship, from how to choose a processor, to what to include in the processing contract and how data is dealt with at the end of that arrangement. It also impacts heavily on the risks associated with processing personal data for both controllers and processors, which in turn affects the contractual risk allocation between those parties.

Under the GDPR, data controllers must carry out a broader due diligence exercise when selecting a processor. Controllers may therefore consider whether it is necessary, or good practice, to carry out a data protection impact assessment before entering into a major new processing arrangement.

Whenever processing is carried out on behalf of a controller by third party, such parties must enter into a written agreement.

The requirements are listed in article 28:

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 processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. 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. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, 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:

    a. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

    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. takes all measures required pursuant to Article 32;

d. respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

e. takes into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

f. assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

g. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

h. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

It is important to note that while processors have some direct obligations, controllers still have more extensive liability than processors under the GDPR. They remain liable for all damage caused by processing which infringes the GDPR, whereas processors are only liable under the GDPR when they breach processor specific provisions or act outside the controller's instructions.

The Scheme currently has no agreements with companies to outsource this data.

Section 13: Article 30 – Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its 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, the controller's representative and the data protection officer;

    b. the purposes of the processing;

    c. a description of the categories of data subjects and of the categories of personal data;

    d. the categories of recipients to whom the personal data has been or will be disclosed including recipients in third countries or international organisations;

    e. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

    f. where possible, the envisaged time limits for erasure of the different categories of data;

    g. where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

    a. the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

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

    c. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

    d. where possible, a general description of the technical and organisational security measures referred to in Article 32 and Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Section 14 Article 32 – Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

    a. the pseudonymisation and encryption of personal data;

    b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

    c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

    d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Section 15- Article 33- Notification of a personal data breach to the supervisory authority

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

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It is potentially very broad. It is not limited to loss of data and extends to unauthorised access or alteration. However, it only captures actual breaches and not suspected breaches.

Where a personal breach occurs as a result of cross- border data processing, or where it will substantially affect data subjects in more than one EU Jurisdiction, this will lead to the use of the one- stop- shop mechanism, as contemplated under Article 60 of the GDPR. This is relevant in the case of banks having multiple establishments across the EU.

Section 16- Article 37 Designation of the data protection officer

The DCS is obliged to appoint a data protection officer.

The role of the data protection officer is to monitor compliance with the Regulation, providing information and advice, and liaising with the supervisory authority.

The data protection officer:

Must report to the highest level of management within the business;

Must be able to operate independently and not be dismissed or penalised for performing the tasks;

The DPO can be assigned other roles as long as these tasks do not give rise to conflict of interests.

The DPO of the Schemes is: **Mr Andrew Sammut**
Tel: 25485339
Email: Asammut@compensationschemes.org.mt