GENERAL DATA PROTECTION POLICY

This Policy describes and provides the required information regarding the handling of personal data by the Office of the Arbiter for Financial Services ("OAFS", "we") and your rights in terms of the applicable Law. This Policy is to be read in the light of the applicable provisions of the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR") and especially Articles 13, 14 and 21.

Scope. Whether the Data Subject ("you") are a complainant, a representative of an applicant, or just want to find out more about the complaint procedure managed by the OAFS, we would like to provide you with an overview of the personal data we collect from you as a financial services redress mechanism and what we use this data for. In addition, we would like to inform you about the entitlements and rights you have under the applicable data protection law.

Definitions. For the purposes of this Policy, the definitions contained in Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR")[1] will apply in like manner, *mutatis mutandis*.

Law. This Policy and any resulting effects are governed by the Laws of Malta and the Courts of Law in Malta have non-exclusive jurisdiction.

Contents

[1] Ref. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

1. Who is responsible for personal data processing and whom can you contact?

The Data Protection Officer ("DPO") for the Office of the Arbiter for Financial Services may be reached on the following addresses:

The DPO
Office of the Arbiter for Financial Services,
First Floor, St Calcedonius Square, Floriana FRN1530. Malta.
[**dpo.oafs@financialarbiter.org.mt**]

2. What personal data does the OAFS process when people contact us?

We record details about your contact with us manually or on an excel worksheet which is saved on servers hosted by MITA, the Malta Government Agency which provides IT infrastructure to all government agencies.

We will use your personal information to provide you with any information or services that you ask for, or to reply to any correspondence exchanged with us. If you have asked us to intervene on a minor case with a financial services provider against whom you have a dispute, we will share such personal information, as is necessary, with such entity solely for the purpose of helping you with your query. Where so required, we will also use personal information to analyse information, what type of questions are being directed to the OAFS, and whether the service we provide is effective in delivering useful information, guidance or otherwise. In other cases, we will endeavour to minimise the use of personal data, as may be applicable and required.

Contacting us by phone. Calls to our office lines may be recorded for quality, evaluation, security and training purposes. When you contact us, we ask for the necessary personal information, as may be applicable, depending on the nature of the call. You are under no obligation to provide this information to us, but it enables us to provide a better quality of service when you contact us again. As a minimum, we will hold your name and phone number for the purposes specified above unless you inform us that you wish to remain anonymous.

Monitoring of emails. Any email sent to us, including any attachments, may be monitored and used by us for reasons of security and for monitoring compliance with security policy. Email monitoring or blocking software may also be used. The site and domain are hosted and managed by the Malta Information Technology Agency (MITA)[2], on behalf of The Office of the Arbiter for Financial Services. MITA has its Head Office registered at:

[2] Ref. https://mita.gov.mt/en/Pages/Contact.aspx

Data Protection Office
Malta Information & Technology Agency
Gattard House, National Road, Blata l-Bajda HMR 9010. Malta.
Telephone (+356) 2599 2410 Email: dp.mita@gov.mt

Please be aware that you have a responsibility to ensure that any email you send to us is within the bounds of the Law.

As a public agency, we are required to produce statistical information about our work. In this regard, we publish annual anonymised aggregated data of the number of enquiries (phone calls and emails) and complaints that we receive and process, including the subject matter of such enquiries. We never publish statistical information which could in any way identify consumers.

In regard to enquiries, once such annual statistical tables are produced, personal details, categorisation of the enquiry and any notes taken describing the enquiry will be destroyed.

In regard to statistical information relating to complaints, our retention policy outlined below applies (refer to question 6 below).

CCTV (Closed Circuit Television)

The OAFS operates a video-surveillance system to deter, prevent, manage and investigate safety and security incidents as well as for the protection of persons, property and documents against damage, theft, intrusion, assault or any other threat. The video-surveillance system complements other typical security and access control purposes by monitoring specific areas and events. It forms part of the measures to support broader OAFS security policies. The system is not used for any purpose other than those mentioned above. For instance, it is not used to monitor the workstations of personnel or attendance. Neither is the system used as an investigative tool for purposes other than those instances described above, or in disciplinary procedures unless a physical security incident or criminal behaviour is involved.

CCTV footage is recorded on a hard-drive and kept on a rolling 30 days. Footage beyond 30 days is automatically deleted.

3. In the case of a Complaint, what personal data does the OAFS process and where does this data come from?

The OAFS processes personal data obtained from the Complaint Forms submitted to it by the Complainant/s and/or their respective representative. In addition, the OAFS processes personal data that is received from the Respondent party/parties, that is, the financial services provider against which the Complaint is lodged.

As part of the procedures, the following personal data is usually processed by us, as follows:

- First and last name/s of consumer/s submitting complaint

- (Correspondence) Address
- Phone number/s
- E-mail address
- Skype ID
- Date and time of the Complaint Registration
- First and last name/s of person assisting or representing the consumer/s, if applicable
- (Correspondence) Address data of the person assisting or representing the consumer/s, if applicable
- Phone number/s of person assisting or representing the consumer/s, if applicable
- E-mail address of person assisting or representing the consumer/s, if applicable
- Details of any person/s who originally sold the product or service to the consumer/s

In addition to the above-mentioned items of personal data, there are other data items that would be required in connection with the Complaint submitted to the OAFS and the subsequent procedures relating to the mediation and/or investigation. Such data and information may relate to any contractual agreement/s you may have entered or signed up to, substantiating documentation directly or indirectly related to such contractual agreement/s, products or services you may have purchased or otherwise subscribed to, on a one off or a continued-delivery basis. In this regard, we may also require the production, from you and/or other parties, correspondence (including voice/video recordings and other media files) that may have passed between you, your representative and/or the Respondent or other relevant third parties.

4. In the case of a Complaint, what is the personal data processed for (purpose of processing) and on what legal basis does this processing take place?

Your personal data will be processed in accordance with the provisions of the General Data Protection Regulation and the Data Protection Act in Malta (Act 20 of 2018, Chapter 586 of the Laws of Malta). The processing of your personal data takes place exclusively to answer queries and properly conduct the necessary work in connection with the Complaint you would have submitted to us, with regard to the applicable complaint procedure/s and in accordance with the rules of procedure relevant and as contained in the applicable Laws.

The substantive legal basis for the processing of your personal data is the Arbiter of the Financial Services Act (Chapter 555 of the Laws of Malta), which attributes the necessary functions, powers and rights to this Office and, in particular, Article 21 (Competence of Arbiter), Article 22 (Procedure relating to complaints), Article 24 (Mediation), Article 25 (Investigation), Article 26 (Adjudication) and Article 27 (Appeal and enforceability).

In line with GDPR Article 6 (1)(f), processing shall be lawful, only if and to the extent that, it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, especially where the processing is carried out by public authorities in the performance of their tasks. This, together with the consent provided by the data subject to the processing of his or her personal data for one or more specific purposes, as per GDPR Art. 6(1)(a) for the

essential legal basis for the data processing activity carried out by the OAFS, in the execution of its mandate.

Furthermore, it is pointed out that in line with L.N. 177 of 2018, Restriction of the Data Protection (Obligations and Rights) Regulations, 2018, and in particular Regulation 4(e), the scope of the obligations and rights provided for in GDPR Articles 12 to 22, 34, as well as Article 5 (as applicable), any restriction to the rights of a data subject shall only apply where such restrictions are a necessary measure for the establishment, exercise or defence of a legal claim and for legal proceedings which may be instituted under any law.

5. Who has access to your personal data?

Your personal data will only be made accessible and transmitted to the parties directly involved in the complaint procedure or which may have a duty or legitimate interest at law to have access to such data and information. Generally speaking, the following will have access to some or all of the personal data pertinent to the said procedures, as follows and at different stages, as may be applicable:

- the personnel acting and serving the OAFS;
- any authorised or specifically engaged party acting for or otherwise assisting the OAFS in the course of proceedings;
- the person who will assist or represent you in the course of the proceedings or that you may have authorised;
- the Respondent and its authorised agents, dependents and (legal) representative/s.

If your case is appealed, the case file is passed on to the Courts of Appeal (Inferior Jurisdiction) in its entirety.

After the decision of the Arbiter becomes *res judicata* (binding on all parties and cannot be pursued any further), if in the Arbiter's opinion there is substantial evidence of any significant breach of duty or misconduct on the part of a financial services provider, or any criminal conduct of any of the parties, the Arbiter shall refer the matter to the competent authorities to take any further appropriate action, if any, according to law.

Furthermore, it is to be noted that it is not excluded that certain duly contracted service providers (data processors within the meaning of GDPR Art. 28) may also have short-term access to your personal data. Such data processors are, in particular, persons responsible for the continued care and maintenance of the implementation of the I.T. infrastructure and security applications at the OAFS, together with service providers in the telecommunications industry (in providing the necessary electronic communication channels), printing and computer hardware services and general logistics. It is to be noted that all relevant providers (processors) will be engaged by virtue of a written contractual agreement that is to cater for the duties and responsibilities around the GDPR.

It is not usual practice for the OAFS to allow its service providers (data processors) to sub-contract to third parties. Should this be the case, the appropriate (contractual) measures will be taken so as to ensure that the sub-processor will assume the responsibilities bestowed by us on the processor, as may be so applicable.

All the above-mentioned parties are to be regulated or otherwise made subject to the applicable provisions of the General Data Protection Regulation and the Data Protection Act in Malta (Act 20 of 2018 of 28 May 2018).

6. For how long will your data be stored?

In line with L.N. 177 of 2018, Restriction of the Data Protection (Obligations and Rights) Regulations, 2018, and in particular Regulation 5(3), it is pointed out that the retention period to be applied for personal data that is processed pursuant to these regulations, shall not be longer than what is necessary for the purpose of the processing of such personal data or shall not be longer than the period required to achieve the aim of the restriction, or as provided by law.

Except for decisions of the Arbiter (see below), physical and electronic (i.e. scanned) case files will be kept by the OAFS for five (5) years from the date when the decision becomes binding on all parties to the complaint.

Once the applicable retention period expires, physical and electronic copies of case records (that is, scanned copies of the physical file) will be destroyed, except for names of the parties and details of the complaint which will be retained to facilitate searches of decisions.

Physical and electronic versions of the Arbiter's decisions as relayed to the parties to the complaint will be retained by us permanently.

Decisions issued by the Arbiter for Financial Services are published on the Office's website and will remain available for a minimum of ten (10) years from the date of the Arbiter's decision. The published version will replace complainants' names with different initials to make them unidentifiable.

We are also obliged to publish a summary of cases decided by the Arbiter in our Annual Report. Here, too, we will replace complainants' names with different initials to preserve anonymity.

7. Are data transmitted to a third country or to an international organisation?

There are no transfers of personal data to countries outside the EU (European Union) / EEA (European Economic Area) or to an international organisation.

As part of the remote maintenance of software and standard I.T. components, especially in the context of certain troubleshooting in individual cases stations or terminals, MITA may make use of an I.T. service provider from a third country outside the EU/EEA (e.g. the USA). Details sourced from MITA will be provided to you separately, as and if required by law.

8. What data subject rights do you have?

In terms of GDPR, consent is not regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. Thus, the Data Subject has the right to withdraw his or 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.

According to GDPR Art. 15 you have the Right of Access to obtain from the Data Controller confirmation as to whether or not your personal data is being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- 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;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling.

In addition, you may, under GDPR Article 16, obtain from the Data Controller, without undue delay, the Rectification of inaccurate personal data about you.

The law also allows for the exercise of other rights, as follows:

- Article 17. Right to erasure ('right to be forgotten'). The data subject shall have the right to obtain from the Data Controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay, depending on the conditions applicable at Law.

- Article 18. Right to restriction of processing. This applies in one or more of the following cases:
  - 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;
  - the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
  - the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
  - the data subject has formally objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

- Article 20. Right to data portability. The right of the data subject to receive his/her personal data (which he/she has provided to a Data Controller) in a structured, commonly used and machine-readable format, and ancillary right to transmit such data to another Data Controller without hindrance.

Please do bear in mind that Data Protection is a civil law right and is not an absolute right law, that is, there are other laws and circumstances which – by their nature – take preference and prevalence over personal data protection, as further detailed in the GDPR and in the relevant body of Laws in Malta (e.g. laws regulated public safety and security, criminal law).

Thus, the Data Subject's rights referred to above are not absolute and there could be situations where the right may either not be exercised or may only be partially entertained by the Data Controller/Processor.

Furthermore, in order to allow the OAFS to adequately conduct its functions at Law, the necessary personal data would need to be processed. Without the right information, the fair and good delivery of service would be prejudiced. In the event of an objection to process your personal data, we will no longer process your personal data, unless it is established that there are compelling legitimate grounds for processing such data, which grounds do outweigh your interests, rights and freedoms, and may be justified as being pursued for the common good.

The above is further substantiated by L.N. 177 of 2018, Restriction of the Data Protection (Obligations and Rights) Regulations, 2018, and in particular Regulation 4(e), where the scope of the obligations and rights provided for in GDPR Articles 12 to 22, 34, as well as Article 5 (as applicable) may be restricted for the establishment, exercise or defence of a legal claim and for legal proceedings which may be instituted under any law. Thus, where any restriction provided for under these regulations applies, the OAFS shall inform the data subject, provided such a disclosure will not be prejudicial to the purposes of the restriction applied pursuant to these regulations.

Data Subject Request (DSR). You may exercise the above-mentioned rights by submitting your request, in writing, including the following items:

- Name and Surname
- Contact Details
- Proof of identification

- Indication whether you have a Complaint lodged with OAFS (and whether such Complaint is pending review)
- Indication whether you are engaged or known to the OAFS, otherwise than as Complainant
- Indication of the GDPR right being exercised

The request is to be sent (manually or electronically) to the attention of the DPO as follows:

The DPO
Office of the Arbiter for Financial Services,
First Floor, St Calcedonius Square, Floriana FRN1530. Malta.
[dpo.oafs@financialarbiter.org.mt]

9. What are the data subject's rights of redress and remedy?

Without prejudice to any other administrative or judicial remedy, GDPR Art. 77 allows every data subject the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy.

The Data Protection Supervisory Authority responsible for the OAFS is:

Information and Data Protection Commissioner
Floor 2, Airways House, High Street, Sliema, SLM 1549. MALTA.
Telephone (+356) 2328 7100 Email idpc.info@gov.mt

In line with GDPR Art. 78 and 79, without prejudice to any other administrative or non-judicial remedy:

- each natural or legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them;
- each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed, as a result of the processing of his or her personal data in non-compliance with this Regulation.

The Data Subject has the right to mandate a not-for-profit body, organisation or association which has been properly constituted at Law, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in this part on his/her behalf, and to exercise the right to receive compensation where provided for by Member State law.

10. Is there an obligation for you to provide your data?

You only need to provide us with the personal data and information required for the adequate completion of your Complaint, or for the processing of your request and the execution of the relevant procedure.

Please be advised that if you withhold or otherwise object to the OAFS processing personal data necessary and required in the consideration of the relevant Complaint or procedures, and in line with the functions and powers of the OAFS, then the OAFS would not be in a position to adequately review and/or decide upon your Complaint. In such a case, the Complaint will be rejected or otherwise abandoned/discontinued.

11. To what extent is there automated decision-making in individual cases?

Automated decision-making within the meaning of GDPR Art. 22, that is, decisions that rely solely on automated processing, including profiling, cannot and are not found in set ups such as the OAFS; it is not the remit of the OAFS to perform such automated processing.

12. Updating of this Policy

From time to time, it is possible that we may need to change or amend this General Data Protection Policy as a result of changes to our operation, changes to the regulatory framework in which we operate and/or changes to the website.

This version of the Policy has been approved on 7 March 2019.