Order of Malta Dial-a-Journey Trust
Data Privacy Policy
May 2018

Data controller

Order of Malta Dial-a-Journey Trust as a data controller is committed to respecting the privacy of personal information which it uses in connection with its day to day activities. Our address is:

17 Munro Road
STIRLING
FK7 7UU

Complaints

If a data subject is concerned about the way we have processed their personal data and wishes to make a complaint or request a review they should write to the Chief Executive, Order of Malta Dial-a-Journey Trust 17 Munro Road STIRLING FK7 7UU email: enquiries@dial-a-journey.org if they are not content with the outcome of their complaint or review, contact:

The Information Commissioner's Office

Head office
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number Fax: 01625 524 510

Scotland-Regional Office
Information Commissioner's Office
45 Melville Street
Edinburgh
EH3 7HL
Tel: 0303 123 1115
Email: scotland@ico.org.uk

Under the GDPR, the data protection principles set out the main responsibilities which we will follow in relation to personal data we processes.

Article 5 of the GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary 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 the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

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."

We collect personal data on lawful grounds as may be necessary for our work as a Trust.

For processing to be lawful under the GDPR, we need to identify a lawful basis before we can process personal data.

It is important that we determine our lawful basis for processing personal data and document this.

Our lawful basis for processing has an effect on individuals' rights. For example, if we rely on someone's consent to process their data, they will generally have stronger rights, for example to have their data deleted.

The GDPR allows member states to introduce more specific provisions in relation to Articles 6(1)(c) and (e):

"(c) processing is necessary for compliance with a legal obligation";
"(e) 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."

These provisions are particularly relevant to public authorities and highly regulated sectors.

Lawful bases for processing personal data and special categories of data are as follows:

Lawfulness of processing conditions

6(1)(a) - Consent of the data subject

6(1)(b) - Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

6(1)(c) - Processing is necessary for compliance with a legal obligation

6(1)(d) - Processing is necessary to protect the vital interests of a data subject or another person

6(1)(e) - 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.

6(1)(f) - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Conditions for special categories of data

9(2)(a) - Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law

9(2)(b) - Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement

9(2)(c) - Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

9(2)(d) - Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

9(2)(e) - Processing relates to personal data manifestly made public by the data subject

9(2)(f) - Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

9(2)(g) - Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards

9(2)(h) - Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

9(2)(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 healthcare and of medicinal products or medical devices

9(2)(j) - Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

Consent

- Consent means offering individuals genuine choice and control.
- Consent requires a positive opt-in. We won't use pre-ticked boxes or any other method of consent by default.
- Explicit consent requires a very clear and specific statement of consent.
- We will keep our consent requests separate from other terms and conditions.
- We will be specific and granular. Vague or blanket consent is not enough.
- We will be clear and concise.
- We will name any third party controllers who will rely on the consent; and
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent - who, when, how, and what we told people.
- Keep consent under review, and refresh it if anything changes.
- Avoid making consent a precondition of a service.
- If we would still process the personal data without consent, asking for consent is misleading and inherently unfair.
- To make 'consent' a precondition of a service is unlikely to be the most appropriate lawful basis.
- Public authorities, employers and other organisations in a position of power over individuals should generally avoid relying on consent as it is unlikely to be freely given.

Children

- The GDPR contains new provisions intended to enhance the protection of children's personal data.
- Where 'Information society services' are offered directly to a child, including most internet services provided at the user's request, we must ensure that a privacy notice is written in a clear, plain way that a child will understand and we must obtain consent from a parent or guardian to process the child's data where they are 13 or under.

The GDPR emphasises that protection is particularly significant where children's personal information is used for the purposes of marketing and creating online profiles.

Documentation

We record the following information:

- name and details of our organisation (and where applicable, of other controllers, our representative and data protection officer);
- purposes of the processing;
- description of the categories of individuals and categories of personal data;
- categories of recipients of personal data;
- details of transfers to third countries including documentation of the transfer mechanism safeguards in place;
- retention schedules; and
- description of technical and organisational security measures

Personal data: your rights

Individuals whose personal data we process have the following rights:

The right to be informed

- The right to be informed encompasses your right to receive 'fair processing information', typically through a privacy notice.
- It emphasises the need for transparency over how we use personal data.

The right of access

- Individuals have the right to access their personal data and supplementary information.
- The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information - this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63).

We will provide a copy of the information **free of charge**. However, we can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

We may **also charge** a reasonable fee to comply with requests for further copies of the same information. This does not mean we can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

Information will be provided without delay and at the latest within one month of receipt.

We are able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, we can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where we refuse to respond to a request, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

We are required to verify the identity of the person making the request, using 'reasonable means'.

If the request is made electronically, we will provide the information in a commonly used electronic format.

Where we process a large quantity of information about an individual, the GDPR permits us to ask the individual to specify the information the request relates to (Recital 63).

The GDPR does not include an exemption for requests that relate to large amounts of data, but we may be able to consider whether the request is manifestly unfounded or excessive.

Right to rectification

The GDPR gives individuals the right to have personal data rectified.

Personal data can be rectified if it is inaccurate or incomplete.

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If we have disclosed the personal data in question to third parties, we will inform them of the rectification where possible. We will also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

We will respond to a request for rectification within one month.

This can be extended by two months where the request for rectification is complex.

Where we are not taking action in response to a request for rectification, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

Right to erasure

- The right to erasure is also known as 'the right to be forgotten'.
- The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:
- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

There are some specific circumstances where the right to erasure does not apply and we can refuse to deal with a request.

We can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

There are extra requirements when the request for erasure relates to children's personal data, reflecting the GDPR emphasis on the enhanced protection of such information, especially in online environments.

If we process the personal data of children, we will pay special attention to existing situations where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forums. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent (Recital 65).

If we have disclosed the personal data in question to third parties, we must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

The GDPR reinforces the right to erasure by clarifying that organisations in the online environment who make personal data public should inform other organisations who process the personal data to erase links to, copies or replication of the personal data in question.

While this might be challenging, if we process personal information online, for example on social networks, forums or websites, we will endeavour to comply with these requirements.

Right to restrict processing

- Individuals have a right to 'block' or suppress processing of personal data.
- When processing is restricted, you are permitted to store the personal data, but not further process it.
- You can retain just enough information about the individual to ensure that the restriction is respected in future.
- We are required to restrict the processing of personal data in the following circumstances:
- Where an individual contests the accuracy of the personal data, we will restrict the processing until we have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task), and we are considering whether our grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- Where we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If we have disclosed the personal data in question to third parties, we will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

We will inform individuals when we decide to lift a restriction on processing.

Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

We must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information will be provided free of charge.

If the individual requests it, we may be required to transmit the data directly to another organisation if this is technically feasible. However, we are not required to adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, we must consider whether providing the information would prejudice the rights of any other individual.

We must respond without undue delay, and within one month.

This can be extended by two months where the request is complex or we receive a number of requests. We must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where we are not taking action in response to a request, we must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Individuals must have an objection on "grounds relating to his or her particular situation".

We must stop processing the personal data unless:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

We must inform individuals of their right to object "at the point of first communication" and in our privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

We must stop processing personal data for direct marketing purposes as soon as we receive an objection. There are no exemptions or grounds to refuse.

We must deal with an objection to processing for direct marketing at any time and free of charge.

We must inform individuals of their right to object "at the point of first communication" and in our privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.

If we are conducting research where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

We must offer a way for individuals to object online.

Rights related to automated decision making including profiling

- The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

Individuals have the right **not to be subject to a decision** when:

- it is based on automated processing; and
- it produces a legal effect or a similarly significant effect on the individual.

We must ensure that individuals are able to:

- obtain human intervention;
- express their point of view; and

- obtain an explanation of the decision and challenge it.

The right does not apply if the decision:

- is necessary for entering into or performance of a contract between us and the individual;
- is authorised by law (eg for the purposes of fraud or tax evasion prevention); or
- based on explicit consent. (Article 9(2)).

Furthermore, the right does not apply when a decision does not have a legal or similarly significant effect on someone.

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work;
- economic situation;
- health;
- personal preferences;
- reliability;
- behaviour;
- location; or
- movements.

When processing personal data for profiling purposes, we must ensure that appropriate safeguards are in place.

We must:

- ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences;
- use appropriate mathematical or statistical procedures for the profiling;
- implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors; and
- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions taken for the purposes listed in Article 9(2) must not:

- concern a child; or

- be based on the processing of special categories of data unless:
- we have the explicit consent of the individual; or
- the processing is necessary for reasons of substantial public interest on the basis of EU / Member State law. This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual.

Contracts

- Whenever we use a processor we will have a written contract in place.
- The contract is important so that both parties understand their responsibilities and liabilities.
- The GDPR sets out what needs to be included in the contract.
- Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected.
- Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

Data breaches

- The GDPR introduce a duty on the Trust to report certain types of data breach to the relevant supervisory authority (the Information Commissioner).
- In some cases, we will also have to report certain types of data breach to the individuals affected.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

We only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals - for example, result in

discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, we will need to notify the ICO about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we must notify those concerned directly.

A 'high risk' means the threshold for notifying individuals is higher than for notifying the ICO.

A notifiable breach has to be reported to the ICO within 72 hours of the Trust becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

International transfers

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations. A transfer, or set of transfers, may be made where the transfer is:

- made with the individual's informed consent;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defence of legal claims;

- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

The first three derogations are not available for the activities of public authorities in the exercise of their public powers.

Our website

Personal information we collect and why we collect it

We collect and use personal information for the following reasons.

Web forms

Should you choose to contact us using a contact form or take part in a public consultation using a web form, the data you supply will be:

- sent to us by secure email
- stored locally by us so that we can deal with your request
- stored temporarily by our website provider, Computer Division Stirling in a secure UK based data centre

We will delete your data in line with our data retention policies.

Other online forms

For some services we use online forms using Microsoft Word. You can print the forms and complete by hand or use Word to complete them on a computer or other device.

If you complete the form on your computer and send it to us by email we will retain and delete your data in line with our data retention policies.

Email links

If you contact us using an email link on our website, the data you supply will be:

- sent to us by secure email
- stored locally by us so that we can deal with your request

We will retain and delete your data in line with our data retention policies.

Our web server

Our website is hosted by One & One in a secure UK based data centre. The data centre has a number of physical security features that restrict access to authorised personnel. There are additional restrictions on access to our web server within the data centre.

We use the latest security technology to deliver the website to your computer and to transfer files between our web server and your computer.

Third party websites

We may use a range of third party websites to provide specialist services and applications. We will apply the same data privacy policy standards to data we collect through these services. We will update this section shortly.

Changes to our privacy policy

We may change our website privacy from time to time to meet legislative or industry requirements. We will use the change log to note change.

Reviewed May 2018