Data Protection Policy

Menter Gorllewin Sir Gâr aims to maximize our obligations under the Data Protection Act 1998. The Chief Executive of Menter Gorllewin Sir Gâr has responsibility for complying with the Data Protection Act and the General Data Protection Regulation.

This data protection policy applies to all personal data we process regardless of the media on which that data is stored if it relates to employees , customers, clients, trustees, suppliers. , shareholders, users of the website or any other data holder.

This data protection policy applies to all company personnel ("you"). You must read, understand and comply with this data protection policy when processing personal data on our behalf. This data protection policy sets out what we expect from you to comply with the relevant law. Your compliance with this data protection policy is mandatory.

Failure to comply with this Policy may result in disciplinary action involving dismissal.

Personal information including personal data in print and on computer is held in relevant filing systems. This information must be accurate and should be updated when necessary and employees, volunteers, job applicants and employees have the right to access the records held about them.

1.1 Principles of personal data protection

We adhere to the principles relating to the processing of personal data set out in the General Data Protection Regulation which requires personal data:

1. Processed lawfully, fairly and transparently.

2. Only collected for specific, clear and valid purposes.

3. Adequate, relevant and limited to what is required in relation to the purposes for which it is processed.

4. Correct and, where necessary, updated.

5. Not kept in bulk format allowing data holders to be identified longer than is necessary for the purposes for which the data is processed.

6. Be processed in a manner that ensures its safety using appropriate technical and organizational measures to protect against unauthorized or unlawful processing and against accidental loss, destruction or damage.

7. Not transferred to another country without appropriate security measures in place.

8. Provided for data holders and the data holders are entitled to exercise certain rights in relation to their personal data.

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

1.2 Legality and fairness

Personal data must be processed lawfully, fairly and transparently in relation to the data holder.

You can only collect, process and share personal and specific data reasonably and lawfully. The General Data Protection Regulation restricts our personal data actions for certain lawful purposes.

These restrictions are not intended to prevent processing, but to ensure that we process personal data fairly and without adversely affecting the data holder.

The General Data Protection Regulation allows processing for specific purposes, some of which are set out below:

(a) the data holder has given his consent;

(b) the processing is necessary for performing a contract with the data holder;

(c) to meet our legal compliance obligations;

(d) to protect the essential interests of the data holder; or

to pursue our legitimate interests for purposes which are not prohibited because the processing prejudices the fundamental interests or rights and freedom of data holders. The purposes for which we process personal data for legitimate interests need to be specified in the relevant privacy notices.

1.3 Consent

A data holder allows us to process their personal data if they clearly show agreement either through a statement or positive steps to the processing. Permission requires positive action so that staying quiet, ticked boxes or inactivity is unlikely to be sufficient. If permission is granted in a document that deals with other matters, then the separate permission must be retained for those other matters.

Data holders must be able to withdraw their consent to the processing easily and at any time, and the wish must be honored promptly. Consent may need to be renewed if you intend to process personal data for a different and incompatible purpose to that disclosed when the data holder had given their consent in the first instance.

Unless we can rely on another legal basis of processing, explicit consent is required for the processing of sensitive personal data, for automatic decision-making and for cross-border data transfers.

We usually rely on another legal basis (where specific consent is not required) to process most sensitive data types. If specific consent is required, you must give the data holder a fair processing notice to collect, express consent.

1.4 Transparency (informing data holders)

The General Data Protection Regulation requires data controllers to provide detailed, specific information to data holders depending on whether the information was collected directly from data holders or elsewhere.

Such information must be provided through appropriate privacy notices and must be concise, transparent, understandable, accessible, and in clear and appropriate language so that a data holder can understand them easily.

Whenever we collect personal data directly from data holders, including for human resources or employment purposes, we must provide all the information required by the General Data Protection Regulation to the data-holder, including the identity of the data controller, how and why we use the data, the process, if we disclose, protect and store that personal data by a fair processing notice.

The fair processing notice is required when the data holder first provides the personal data.

When personal data is collected indirectly (for example, by a third party or a publicly available source), you must provide the data holder with all the information required by the General Data Protection Regulation as soon as possible. possible after collecting / receiving the data.

You must also check that the personal data is collected by the third party in accordance with the General Data Protection Regulation and on a basis that reflects our proposed processing.

1.5 Purpose restriction

Personal data must only be collected for specific, clear and valid purposes. It should not be further processed in any manner incompatible with those purposes.

You may not use personal data for new, different or incompatible purposes. What was disclosed when it was first obtained Unless you have notified the data holder of those new purposes and they have consented to them where necessary.

1.6 Reduce data

Personal data must be adequate, relevant and limited to what is required in relation to the purposes for which it is processed.

You can only process personal data if it is part of your job duties to do so. You cannot process personal data for any reason that is not related to your job.

Personal data can only be collected for your job: do not collect excessive data and do not make unnecessary copies. Ensure that any personal data collected is adequate and relevant to the purposes intended.

You must ensure that when personal data is no longer required for specific purposes, it will be deleted, securely destroyed or anonymised in accordance with our data retention guidelines.

1.7 Accuracy

Personal data must be accurate and, where necessary, updated. It must be corrected or removed promptly when it is wrong.

You will ensure that the personal data we use is to be accurate, complete, up to date and relevant to the purpose for which it was collected. You must check the accuracy of any personal data at the collection point and regularly thereafter. You must take all reasonable steps to destroy or amend incorrect or non-current personal data.

1.8 Storage restriction

Personal data should not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not hold personal data in a form that allows the data holder to be identified for longer than is necessary for legitimate business purposes or purposes that we originally collected, including for the purposes of meeting any legal requirements, accounting or reporting.

We will maintain retention policies and procedures to ensure that personal data is removed after reasonable time for the purposes for which it is conducted, unless law requires such data to be kept for a minimum period.

You will take all reasonable steps to destroy or remove all personal data from our systems which is no longer required in accordance with all our relevant policies. This includes asking third parties to delete such data where relevant.

1.9 Protection of Personal Data

Personal data must be obtained through appropriate technical and organizational measures against unauthorized or unlawful processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to the size, scope and business, the resources available to us, the amount of personal data we own or maintain on behalf of others and risks identified (including use of encryption and pseudonyming where applicable).

We will regularly evaluate and test the effectiveness of those safeguards to ensure the safety of our personal data processing.

You are responsible for protecting the personal data we hold. You must take reasonable and appropriate safeguards against unauthorized or unauthorized personal data processing, and against accidental loss or damage from personal data.

You must exercise certain care in protecting sensitive personal data from unauthorized loss, access, use or disclosure. Specifically this includes:

(a) a prohibition on saving personal data to personal computers or other devices;

(b) seek permission from the data controller before any personal data is removed from our site;

(c) use strong passwords;

(d) lock computer screens;

(d) ensure that documents containing personal data and sensitive personal data are kept securely;

(f) encryption of data by electronic transmission to other parties; and

(e) consider the use of separate keys / codes to denote data so that the data holder cannot be identified.

You must follow all the procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the place of destruction.

Personal data can only be passed to third party service providers who agree to comply with the required policies and procedures, and agree to put in place adequate measures, as required.

You must protect data by ensuring the confidentiality, integrity and availability of personal data, as follows:

• Confidentiality means that only people who need to know and authorize the personal data can access it.

• Integrity means that personal data is accurate and fit for the purpose for which it is processed.

• Availability means that authorized users can access the personal data when they need it for authorized purposes.

You must comply

1.11 Data Holder's rights and applications

Data holders have rights when it comes to how we handle their personal data. These include rights to:

(a) withdraw consent to process at any time;

(b) receive specific information about data controller processing activities;

request access to the personal data we hold about them;of personal data.

1.10 Reporting Personal Data Breaches

The General Data Protection Regulation requires data controllers to notify any relevant breaches of personal data to the relevant regulator and, in some cases, the data holder.

If you know or suspect that a breach of personal data has occurred, do not attempt to investigate the matter yourself. Contact the data controller immediately.

1.11 Data Holder's rights and applications

Data holders have rights when it comes to how we handle their personal data. These include rights to:

(a) withdraw consent to process at any time;

(b) receive specific information about data controller processing activities;

(c)request access to the personal data we hold about them;

(d) prevent our use of their personal data for direct marketing purposes;

(e) require us to remove personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to correct inaccurate data or to complete incomplete data;

(f) limit processing in certain circumstances;

(g)challenge justified processing on the basis of our legitimate interests or in the public interest;

(h) request a copy of the agreement allowing the transfer of personal data outside the EEA ',

(i)opposing decisions made based solely on automatic processing, including profiling;

(j) suspension of processing likely to cause damage or distress to the data holder or any other person;

(k) be informed of breaches of personal data which are likely to result in a high risk to their rights and freedoms; complain to the supervisory authority; a

(l) in limited circumstances, accept or require the transfer of their personal data to a third party in a commonly used and structured format.

You must check the identity of a person requesting data under any of the rights listed above (do not allow third parties to persuade you to disclose personal data without proper authorization).

You must send any data holder's request to the Chief Executive immediately.

Please note that it is an offense to hide or destroy personal data which is part of a data holder's access request. Such behavior would also involve gross misconduct under our disciplinary procedure, which could lead to your dismissal.

1.12 Accountability

We have adequate resources and controls in place to ensure and document our compliance with the General Data Protection Regulation, including:

(a) appoint a suitably qualified data controller (where necessary) and an accountant liable for data privacy;

(b) implement privacy through a scheme when processing personal data and complete a Data Protection Impact Assessment Where processing presents a high risk to the rights and freedoms of data holders;

(c) integrate data protection into internal documents including this data protection policy;

(d) train our personnel on the General Data Protection Regulation; a

(e) regularly test the privacy measures implemented and carry out periodic reviews and audits to assess compliance, including the use of test results to demonstrate effort to improve compliance.

1.13 Record keeping

The General Data Protection Regulation requires us to keep full and accurate records of all data processing activities.

You must keep accurate corporate records that reflect our processing, including records of data holder's consent and procedures for obtaining consent.

1.14 Audit

You must regularly review all systems and processes under your control to ensure that they comply with this data protection policy and check that there are adequate governance controls and resources in place to ensure the correct use and security of personal data.

1.15 Privacy Through Data Protection Plan and Risk Assessment

We are required to implement privacy measures by scheme in the processing of personal data by implementing appropriate efficient technical and organizational measures (such as pseudonyms), to ensure compliance with data privacy principles.

You must assess what privacy measures are through a scheme that can be implemented on each program / system / process that processes personal data by taking into account the following:

(a) the most current ways of doing so;

(b) the cost of operating;

(c) the nature, scope, context and purposes of the processing; a

(d) the risks and severity the processing causes against the rights and freedoms of data holders.

You should carry out a Data Protection Risk Assessment (and discuss your findings with the data controller) when implementing major programs or business change programs including processing personal data including:

• the use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes); automatic processing including profiling; large scale sensitive data processing; and systematic monitoring of a large-scale publicly accessible area.

1.16 Direct marketing

We are subject to certain rules and private laws in marketing to our customers.

For example, electronic direct marketing requires the prior permission of a data holder (for example, by email, text or automatic calls).

There is a limited exemption for existing customers called “soft opt in” allowing organizations to send marketing messages or emails if they have received contact details when providing that person's service, where they market similar products or services, and the opportunity for a person to opt out of the marketing when collecting the details first and in all subsequent messages.

The right to object to direct marketing must be specifically offered to the data holder so that it can be clearly distinguished from other information.

Data holder's opposition to direct marketing must be honored. If a customer chooses to come out at any time, their details should be suspended as soon as possible. Prevention means keeping little information to ensure that you can respect the individual's future marketing choices.

1.17 Sharing Personal Data

Generally, we are not permitted to share personal data with third parties unless certain safeguards and contractual arrangements are in place.

The personal data we hold may only be shared with another employee, agent or representative of our group if the recipient has a job related need to know the information and the transfer complies with any relevant cross-border transfer restrictions.

The personal data we hold can only be shared with third parties, such as our service providers, if:

(a) they need to know the information for the purpose of providing the contracted services;

(b) that the sharing of personal data complies with the privacy notice provided to the data holder and if necessary, the data holder's consent has been obtained;

(c) the third party has agreed to comply with the required safety standards, policies and procedures and put in place adequate safeguards;

(d) the transfer complies with any relevant cross-border transfer restrictions; a

(d) a full written agreement containing third party clauses approved under the General Data Protection Regulation has been secured.

1.18 Changes to this Data Protection Policy

(f) We reserve the right to change this data protection policy at any time so check back regularly to obtain the latest copy of this data protection policy.

(g) This Policy was approved by the Menter Gorllewin Sir Gâr Management Committee in January 2019 and signed on their behalf:


The policy will be reviewed in full January 2020