GEMACARE LIMITED

1 Cronk Aust, Andreas Road, Aust, Isle of Man IM7 4EF .
Telephone: (07624) 376800
www.gemacare.co.uk
Email: enquiries@gemacare.co.uk

DATA PROTECTION & CONFIDENTIALITY POLICY

(GDPR)

Policy Review - History:
Please be aware that a hard copy of this document may not be the latest available version, please contact us for the latest version which supersedes all previous versions.

Those to whom this policy applies are responsible for familiarising themselves periodically with the latest version and for complying with policy requirements at all times.

Effective from:	**Replaces:**	**Originator:**	**Page X of Y**
March 2023	Draft Version 2011		1 of 16
Management Team Approval:			
Union the Union & Unison Union Agreement:		N/A	
Ratification:		March 2023	

History or Most Recent Policy Changes – MUST BE COMPLETED		
Version:	Date:	Change:
1.0	February 2019	

CONTENTS:

1. Introduction

This policy sets out the way in which GemaCare Limited; known as “The Company” will collect, store, manage and share private personal information about the people for whom it provides a service and with whom it works. Because of the activities and functions undertaken by the company it may be necessary to use personal information for reasons beyond why the data was collected, for example, safeguarding, emergencies or to prevent a crime..

It is a general principle of the Companies Data Protection Policy that private information will be treated with respect and at a level of confidentiality appropriate to the type of information and the reason it is used. This general expectation of confidentiality should apply in all cases except where it is shared to meet a legitimate function of the Company such as a legal obligation, or in the interests of the person themselves.

This policy is made up of a number of documents. These documents will be updated on a regular basis following any organizational change where the use of personal data has changed e.g. introduction of a new service.

Documents that make up this policy include the following: -

Data Protection Policy (this document)
Privacy Policy
Records Management Policy
Information Security Policy

This policy will also reference the legislation. A link to the legislation can be found on the Information Commissioners website: -

www.inforights.im

The legislation is made up of articles; each of these articles reference a particular focus of the legislation. The articles are supported by a number of recitals that explain the reasoning behind a decision, these are very useful for reference and understanding.

The www.Inforights.im website also contains several useful guides around specific data topics.

The UK website https://ico.org.uk/ is also an excellent website for reference material in relation to the legislation.

The following website has an excellent interaction version of the EU Legislation.

https://gdpr-info.eu

2. Requirements of Legislation & Definitions

The chief requirements outlined in this policy are based upon the 2018 Data Protection Regulation (GDPR), which is the central piece of legislation covering security and confidentiality of personal information.

The DPA imposes obligations on the use of all personal information held by organisations such as the Company. The act contains a number of important definitions which are set out below. It is important to understand these definitions as they will be used in this policy.

Data Protection Legislation: The Isle of Man Data Protection Act 2018

Personal data: The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.

If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive Personal data: The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).

The special categories specifically include genetic data and bio-metric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offenses are not included, but similar extra safeguards apply to its processing (see Article 10).

Data Subject:
An identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as name, identification number, location data, online ID, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person.

Confidential Information:
Information (whether or not recorded in documentary form, or stored on any magnetic or optical disk or memory) relating to the business, products, affairs and finances of the Company for the time being confidential to the Company and trade secrets including, without limitation, technical data and know-how relating to the business of the Company or any of its business contacts, including in particular (by way of illustration only and without limitation).

Data Controller:
The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; GemaCare Limited is a Data Controller.

The **data controller** determines the **purposes** for which and the **means** by which personal data is processed. Employees processing personal data within the organisation do so to fulfill your tasks as data controller.

Data Processor:
A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Joint Data Controller:
The Company is a **joint controller** when together with one or more organisations it jointly determines 'why' and 'how' personal data should be processed. Joint controllers must enter into an arrangement setting out their respective responsibilities for complying with the GDPR rules. The main aspects of the arrangement must be communicated to the individuals whose data is being processed. An example for the Company would be with Emergency Services where information needs to be shared for the welfare of a person.

Data Protection Officer ('DPO'):
The DPO will assist Managers and staff to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

Data subjects shall have the right to contact the Company on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.

Information Commissioners Office (ICO):
The Information Commissioner is the independent authority responsible for upholding the public's information rights and promoting and enforcing compliance with the Island's information rights legislation, which includes the Freedom of Information Act, Data Protection Act and Unsolicited Communications Regulations.

3. Data Protection Principles

The Company processes personal data in accordance with the following data protection principles:

- The Company processes personal data lawfully, fairly and in a transparent manner
- The Company collects personal data only for specified, explicit and legitimate purposes
- The Company processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- The Company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate data is rectified or deleted without delay
- The Company keeps personal data only for the period necessary for processing
- The Company adopts appropriate measures to ensure that personal date is secure, protected against unauthorised or unlawful processing, accidental loss, destruction or damage

How the Company complies with the data protection principles is detailed in the Companies Privacy Policy,

These policies are available on request.

Managers are responsible for ensuring that their Department or Section is adhering to the Policies.

The DPO should be consulted for approval in all cases where a privacy notice is to be used.

4. GemaCare Limited

The management team has overall responsibility for data protection within the Company.

The implementation of this policy is overseen by the Companies Data Protection Officer (DPO). This role is currently assigned to Julie Mattin, who has the responsibility for ensuring it is implemented and operated correctly across the Company.

The DPO is also responsible for investigating incidents involving breaches or potential breaches of information security, Data Protection notification and providing advice.

Whilst the DPO has the responsibilities outlined above**, all senior staff** are responsible for ensuring that this policy is communicated and implemented across their area of responsibility.

The senior staff are responsible for the quality, security and management of personal data in use in their area including carrying out risk assessments and providing reports for the DPO on measures taken to mitigate or deal with information risks. Advice or assistance regarding this policy or the Data Protection Act in general is available to them from the DPO. Excellent guidance is also provided by the Office of the Data Protection Supervisor on their website at https://www.inforights.im/

Training will be provided where required, this can be processed in line with the Companies training programme/staff development review.

All data subject requests are to be reported to the DPO, they should be complied with by the Department or Section processing the relevant data. The DPO will provide advice and guidance as necessary. The process is outlined in Appendix A.

Where personal data is shared by the Company for specific purposes with other organisations, Information Sharing Agreements will be prepared by the appropriate officer and signed on behalf of the Directors by the DPO. Advice can be provided by the DPO.

All data protection and information related breach incidents should be reported immediately to the DPO and managed according to the Companies Data Protection Breach process. The breach reporting process is detailed in Appendix B.

All correspondence with the Information Commissioner's Office on data protection matters will be dealt with by the DPO.

This Policy will be reviewed annually by the DPO to coincide with the annual requirement to notify the Office of the Data Protection Supervisor, and when appropriate to take into account lessons learned from any actual or potential data protection or confidentiality breaches, changes to legislation or guidance from the Information Commissioners Office.

4.1. Staff Training and Awareness

Training will be provided to all employees about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Employees whose roles require regular access to personal data, or who are responsible for implementing this policy, or are responding to subject access requests under this policy, will receive additional training.

The Data Protection Officer will send out regular communications to all staff in relation to data protection awareness.

4.2. Annual Notifications to ICO

The Company must provide an annual notification (on the 31st March each year) to the ICO, summarising the purposes for which data is used by the organisation. This process is known as notification. Failure to submit the annual notification or to keep it up to date is a criminal offence.

The DPO is responsible for submitting the notification. All senior staff must carry out an annual review of their data use and notify the DPO if the type of personal data their Department holds or the way it is managed changes significantly. The DPO will send out an annual reminder of this process.

4.3. Managing the Rights of the Data Subject

Under data protection law the data subject has a number of rights in relation to the personal information that is held about them. These include:-

Right of Access and Subject Access Requests (SAR)
A data subject has the right to ask for copies of personal information held relating to them. This right always applies. There are some exemptions, which will be evaluated on submission of the request.

Right to Rectification
A data subject has the right to ask for information to be rectified if they think it is inaccurate. They also have the right to ask for information they think is incomplete to be completed.

Right to Erasure
A data subject has the right to ask for their personal information to be erased in certain circumstances. Only data that is no longer required for the purposes it was collected should be deleted and therefore it is very unlikely that The Company would ever hold such data. This will always be reviewed by the DPO for validity.

Right to Restriction of Processing
A data subject has the right to ask for the processing of information to be restricted in certain circumstances.

Right to Data Portability

This applies to information supplied to The Company by the data subject. A data subject has the right to ask for the information they gave us to be transferred to another organisation or supply it direct to them.

The above rights will come to The Company as formal requests, definitions of these requests can be found in the Companies Privacy policy.

This section defines how The Company will process the requests from the data subject.

A data subject has the right to make these requests only for data relating to themselves. No request should be processed if there is a possibility that by performing the task another individual can be identified. Refer to the The Company for guidance on specific cases.

There are a number of clear rules and guidelines that relate to these requests:

- There is no fee **
- Requests must be replied to within one month (if a request is complex the Company can extend the time period for responding by a further two months)***
- If the request is made electronically the response must also be issued electronically
- There is no set format for a request, however the Company will assist by provided formatted forms/e-forms
- The response may also provide the following information (depending on the type of request)**:**
    - the purposes of processing;
    - the categories of personal data concerned;
    - the recipients or categories of recipient disclosed the personal data to;
    - retention period for storing the personal data or, where this is not possible, criteria for determining how long it is store;
    - the existence of their right to request rectification, erasure or restriction or to object to such processing;
    - the right to lodge a complaint with the ICO or another supervisory authority;
    - information about the source of the data, where it was not obtained directly from the individual;
    - the existence of automated decision-making (including profiling); and
    - the safeguards provided if personal data is transferred to a third country or international organisation.

* Where the request is manifestly unfounded or excessive The Company may charge a “reasonable fee” for the administrative costs of complying with the request. The Company can also charge a reasonable fee if an individual requests further copies of their data following a request. The fee must be based on the administrative costs of providing further copies.

The Company can extend the time to respond by a further two months if the request is complex or a number of requests have been received from the individual. The Company must let the individual know within one month of receiving their request and explain why the extension is necessary.

Making the request

Although there is no requirement to fill out an official form to submit an SAR, the Company has provided a form to make the submission of a request easier.

Regardless of the format used, the following information should be provided to identify the individual and assist with the search:

- Full name, title and date of birth.
- Current address and previous addresses (reasonable for identification purposes only)
- Specific details of the request, e.g., for an SAR request not all requesters will require all data
- Any other data that may assist in the identification of the individual or the data required e.g. Account numbers, previous names etc.

Before a request can be processed the individual must prove who they are. The standard approach to verification of identity will be in the form of 2 forms of ID:

- One must be a Utility bill issued in the last 3 months
- One must be a form of photo ID, either driving license or passport

If the person does not have any of the above then the request should be reviewed by the Company to identify other possible forms of acceptable identification.

In certain circumstances The Company may be satisfied that the individual is known to them and this level of identification will not be required e.g., an ongoing professional relationship.

Exemptions to the ID process exist for employees, please see the GDPR Policy for specific details.

Although the Company will publish contact details for submitting a request (see Privacy Policy) a request can come in through any team member directly in any format.

Third Party Requests

The GDPR legislation does not prevent an individual from making a request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, The Company need to be satisfied that the third party making the request is entitled to act on behalf of the individual and it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

If processing personal information for criminal law enforcement purposes, the rights of the data subject are slightly different.

4.4. Breach Reporting

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party

- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data (system failure)

Typical real world examples may include:-

- Sending unencrypted data within an email to the wrong person
- Losing a USB stick containing personal data
- Leaving print outs containing personal data In a public area
- Sending a letter to the wrong person
- Computer systems being hacked

The legislation requires any data breach to be reported to the Information Commission within **72 hours** of the breach being reported/identified.

When a personal data breach has occurred, it is necessary to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then The Company must notify the ICO; if it is **unlikely then it does not have to be reported.**

However, if it is decided that the breach does not need to be reported this decision needs to be justifiable therefore, it needs to be documented.

In the event of any suspected breach it should be reported immediately to the Data Protection Officer.

To assist with the documenting and identification of the data breach a Data Breach Reporting Form is attached (Appendix B).

4.5. Information Security

The Company Information security process is defined with the Information Security policy.

4.6. Records Management

The Companies records management responsibilities are defined in the Companies Records Management Policy.

4.7. Data Protection Impact assessments (DPIA's)

It is important that when engaging with a new project, changes to the way that we manage personal data are taken into consideration.

A DPIA is a way to systematically and comprehensively analyse processing and help identify and minimise data protection risks. You can think of it as an audit of the process that highlights any risks to personal data.

DPIAs should consider compliance risks, and also the broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm to individuals, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals (Risk Assessment).

A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. An effective DPIA can bring broader compliance, financial and reputational benefits, helping to demonstrate accountability and building trust and engagement with individuals.

In the very first instance of change all Staff should be thinking about the possible impact on personal data. If it is considered that personal data will be impacted in any way then it is advisable to contact the DPO.

A full DPIA review is only required should there be significant high risk to personal data.

The Company has the right to submit the DPIA to the Information Commission should it feel concerned about the level of risk. The Information Commission will give direction on mitigating actions that can be taken to reduce the identified risks; in rare cases the ICO may decide that the processing is not appropriate. This is unlikely.

4.8. Data Protection 'Privacy by Design'

Data protection 'privacy by design' is another new requirement of the new legislation.

It is very tightly linked to the DPIA assessments in as much as it requires us to consider the privacy requirements of data in all things that we do, this includes existing systems/processes and new processes/systems.

This is very much a requirement of the organisation as a whole. The legislation is really trying to make sure that organisations change their culture and start to include the 'thinking about privacy' actions in everything they do.

Where a change is identified as a higher risk, consideration should be given to the DPIA process.

Not considering a change in this way may risk not carrying out the necessary review; ultimately this could result in GPDC operating unlawfully. It is important to embed this new thought process into everything we do.

The Company will achieve this through by continuous personal and staff development and training.

5. Data Accuracy

Managers are responsible for ensuring that data collected from or about data subjects is complete and fit for purpose.

Staff using Information systems including databases and manual filing systems should receive specific training from their manager (or an appropriate officer nominated) on their use to ensure that information which is required to make decisions about people is accurately and adequately recorded. Standard glossaries and explanations of abbreviations should be available, especially when information is shared between teams and departments.

Wherever a hybrid system of manual and computer records are used in a single environment, guidance must be produced to ensure that staff understand how and when to record information on either or both systems. The purpose of both systems must be clear and understood.

Staff must ensure that personal data held in any form is accurate and up to date. Data subjects should regularly be consulted about whether the information held about them is still current. This will be dependent on the process and the reasons as to why the data is being held. Please refer to the DPO for further guidance.

Application forms and other data gathering tools and processes should be reviewed regularly to ensure that they still gather sufficient information, and do not contain questions which are no longer relevant.

Staff should notify the DPO if personal data is to be used for a new purpose which is materially different to that for which it was obtained, in order to consider whether the use is valid.

5.1. Audit and control

The Company will conduct periodic compliance audits of major services and processes to ensure that this policy and the Data Protection Act are complied with.

Any questions relating to this policy should be directed to the Data Protection Officer.

6. Privacy Statements

It is important that at any point where data is collected the Companies privacy policy is referenced.

There is an additional statement to be added when collecting data from third person e.g., when another individual's details are provided by somebody else. Family member, friend.
These statements are attached (Appendix C).

7. APPENDIX A

See separate document

8. APPENDIX B

Information Breach Report Form

This form is for managers to complete following the initial report of an information incident. It should not take more than 15 minutes to complete.

If you are unsure about the procedures for managing an information incident you should refer to the Data Protection policy.

Please provide as much information as possible. If you do not know the answer or you are waiting on the completion of further enquiries please state this and indicate when this information may be available. In addition to completing the form below, please provide any other supporting information that maybe relevant. If you are unsure about anything then contact the DPO in the first instance.

Should there be an information incident, swift containment and recovery of the situation is vital. Every effort should be made to minimise the potential impact on affected individuals, details of the steps taken to achieve this should be included in this form.

Please do not delay in sending this form to the Data Protection Officer.

Contact Details

Please provide your full name, please note that all information will be kept confidential in relation to this breach report and any further actions.

Full Name	
Phone	
E-mail address	

a) Details of the information incident

a.1. Please describe the incident/breach in as much detail as possible.
a.2. Please give details of when the incident/breach happened. Please note data and time where possible, if there are multiple incidents please detail all dates.
a.3. If there has been a delay in reporting the incident to the DPO please explain why.
a.4. What were the control factors in place to prevent this from happening, it there were none then please state ‘none’.

b) Personal data placed at risk

b.1. What, if any, personal data has been placed at risk? Please specify if any financial, commercial or personal sensitive data has been affected and provide details of the extent.
b.2. How many individuals (Data subjects) have been affected?
b.3. Have the affected individuals been made aware that an incident has occurred? Please state whether their awareness was ‘formal’ e.g., informed them directly or ‘they have discovered through other means’ that their data was compromised.

a.4. What are the potential risks, consequences and adverse effects on those individuals?

a.5. Have any of the affected individuals complained about the incident and if so, what action has been taken?

c) Containment and Recovery

c.1. Has any action been taken to minimise/mitigate the effect on the affected individual(s)? If so, please provide details.

c.2. Has the information placed at risk now been recovered? If so, please provide details of how and when this occurred.

c.3. Have any steps been taken to prevent a recurrence of this incident? If so, please provide details.

c.4. Who have you informed about the incident, internally and externally? For example, in the event of theft, have the Police been informed and do you have a crime number?

d) Training and Guidance

d.1. Please confirm that all employees involved with the incident have successfully completed the Data Protection training?

d.2. Has any additional Information relating to Governance training been provided? If so, please provide details.

d.3. Has any specific detailed operational guidance been developed and provided to staff on handling information, including the use of IT equipment? If so, please provide details.

e) Investigation (may not yet be done)

e.1. What, if any actions have been taken to preserve evidence and/or create an audit trail relating to the information incident?

e.2. What, if any, remedial actions have been taken since the information incident occurred to prevent any recurrence?

e.3. Where remedial actions have been identified what timescales have been agreed for implementation? Please provide details.

e.4. Where remedial actions have been identified what timescales have been agreed for implementation? Please provide details.

What happens next?

When the form is received, the DPO will contact you to provide:

- An incident reference number; and
- Information about our next steps and further information that may be required for the investigation

9. APPENDIX C

Standard Privacy Statement

“The Company collects personal data in accordance with the relevant data protection legislation. Should you wish to learn more about this please read our Privacy Policy which clearly sets out what personal information is collected, why, and for how long. The Privacy Notice can be read on our website or sent to you via email”.

Additional Statement When Collecting Additional Person’s Data

“When you provide us with information about another person on a lawful basis for processing this personal information that is necessary for compliance with a contract and/or legal obligation, that it is necessary for the performance of a task carried out by the Company”