Gallinet Limited
GDPR Compliance Statement & Policy

Context and overview

At Gallinet, we are committed to our obligations for GDPR compliance on three fronts: our responsibilities as an organisation that processes personal data; our role as a data processor on behalf of our clients; and our dedication to providing the very best software.

Gallinet Limited needs to gather and use certain information about individuals through the normal course of business. Gallinet will process individual data subject's information on behalf of our clients. We take the personal and commercial sensitivity of this data very seriously and have processes in place to ensure that data is safe and secure in our care. This includes (but not limited to) data used for testing and project planning, data for migrations/transfers and data used through the provision of technical support.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data is collected, handled and stored to meet the company's GDPR legal requirements — and to comply with the law.

Why this policy exists

This data protection policy ensures Gallinet Limited

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully, it must also not be retained without good cause.

The law is underpinned by important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

The above applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR requirements. This can include, but is not limited to:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Photographs
- Personal files, copies of personal documentation

Data protection risks

This policy helps to protect Gallinet Limited and its clients from data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Gallinet Limited has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The board of directors is ultimately responsible for ensuring that Gallinet Limited meets its legal obligations. These are:

- Being aware of data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Gallinet Limited holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

The IT manager is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards and legal obligations.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

The marketing manager is responsible for:

- Approving any statements attached to communications such as emails and letters.
- Addressing any queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by sound principles.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Gallinet Limited will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally unless specifically authorised.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager if they are unsure about any aspect of data protection.

Data storage

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not in use, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to Gallinet Limited unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

The law requires Gallinet Limited to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Gallinet Limited should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Gallinet Limited will make it easy for data subjects to update the information Gallinet Limited holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by Gallinet Limited are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at support@gallinet.com. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Gallinet Limited will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

Gallinet Limited aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

Client's data storage.

Gallinet provides a workforce management software application called Peoplehours™ to its clients and the following points are noted:

For our clients using the Gallinet Peoplehours™ software, your data is stored in UK-based and certified data centres, operated by FastHosts and UKFast with support from experts who understand your software.

We take care of the database servers, with corporate-standard reliability assured through regular maintenance, software upgrades, bug fixes, virus protection, patches and backups carried out on your behalf. The data centres themselves are in secure, disaster-resistant locations and we are proud to report 99.99% uptime.

The Gallinet Peoplehours™ service employs the following security principles:

- Asset protection – Data is protected against physical tampering, loss, damage or seizure by physical on-site security.
- Separation between clients – Each client has their own database and security is in place to separate one Gallinet client from another.
- Operational security – Gallinet and our service partners have processes and procedures in place to ensure the operational security of the service.
- Identity and authentication – Access to the service is constrained to authorised individuals using password security.
- Audit information – Audit records are kept to enable the monitoring of server access.

Gallinet regularly carries out manual and automatic network penetration testing of our cloud environment using third party testers. Our network is under continuous management and is subject to regular vulnerability scans.

Encrypted restorable backups are made at regular intervals. Gallinet has a disaster recovery plan in the event of a total loss of the data centre.

Gallinet does not share clients' data with any third parties without our clients express instruction. Any such data transfer between organisations will always be in accordance with GDPR standards and our own documented processes.

In the event of a data breach, Gallinet has processes in place to report a data breach to our clients and where necessary, the ICO within 72 hours of discovering the breach. Our first priority will be to restrict the risk and minimize the impact on the individuals and organisations concerned. Responsibility for a breach will be determined once the circumstances are understood.

Client's data within Peoplehours™.

- Gallinet has no direct knowledge or sight of the data as entered by the client.
- Gallinet will not access the client's data unless so required for the performance of the service contracted.
- Gallinet clients using Peoplehours™ are wholly responsible for
    - The type of data that is stored, its accuracy and how it is used.
    - Gallinet will provide tools within the application that will allow data to be deleted or made anonymous so that it is no longer connected to an individual identifiable person.
    - Clients can additionally make requests to Gallinet at any time for any data to be deleted so as to meet requests for rights to be forgotten.
        - Such requests should be in writing, detailed and specific.
- At the conclusion / termination of the business relationship with Gallinet the all the client's data including any backup copies will be wholly and irreversibly deleted within 6 months.

DATA BREACH POLICY

1.0 Introduction

1.1 Gallinet holds a large amount of personal data, a valuable asset that needs to be suitably protected.

1.2 Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

1.3 Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

2.0 Purpose

2.1 Gallinet is obliged under GDPR regulations to have in place a framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

2.2 This Policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents throughout the company.

3.0 Scope

3.1 This Policy relates to all personal and sensitive data held by Gallinet regardless of format.

3.2 This Policy applies to all staff. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of Gallinet.

3.3 The objective of this Policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

4.0 Definition / Types of Breach

4.1 For the purpose of this Policy, data security breaches include both confirmed and suspected incidents.

4.2 An incident in the context of this Policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the company's information assets and/or reputation.

4.3 An incident includes but is not restricted to, the following:

4.3.1 Loss or theft of confidential or sensitive data or equipment on which such data is stored : (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record) Equipment theft or failure

4.3.2 Unauthorised use of, access to or modification of data or information systems Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
4.3.3 Unauthorised disclosure of sensitive / confidential data Website defacement
4.3.4 Hacking attack
4.3.5 'Blagging' offences where information is obtained by deceiving the organisation who holds it

5.0 Reporting an incident

5.1 Any individual who accesses, uses or manages the companies information is responsible for reporting data breach and information security incidents immediately to the GDPR Officer and internally via Support@Gallinet.com.
5.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.
5.3 The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process.
5.4 All staff should be aware that any breach of the Data Protection regulations may result in the companies disciplinary procedures being instigated.

6.0 Containment and Recovery

6.1 The IT Director will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.
6.2 An initial assessment will be made in liaison with relevant staff to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach).
6.3 The lead investigator will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.
6.4 The lead investigator will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.
6.5 Advice from experts across the company may be sought in resolving the incident promptly.
6.6 The lead investigator, in liaison with the relevant other staff will determine the suitable course of action to be taken to ensure a resolution to the incident.

7.0 Investigation and Risk Assessment

7.1 An investigation will be undertaken immediately and wherever possible within 24 hours of the breach being discovered / reported.
7.2 The lead investigator will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.
7.3 The investigation will need to take into account the following:
7.3.1 The type of data involved and its sensitivity
7.3.2 The protections are in place (e.g. encryptions)

7.3.3 what's happened to the data, has it been lost or stolen
7.3.4 Whether the data could be put to any illegal or inappropriate use
7.3.5 Who the individuals are, number of individuals involved and the potential effects on : those data subject(s) : whether there are wider consequences to the breach

8.0 Notification

8.1 The lead investigator, in consultation with the company directors and the director of IT will determine who needs to be notified of the breach.
8.2 Every incident will be assessed on a case by case basis.
8.3 Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the company for further information or to ask questions on what has occurred.
8.4 The company will consider notifying third parties such as their clients, the police, insurers, bank or credit card companies. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.
8.5 The company will consider whether the directors should prepare a press release ready to handle any incoming press enquiries.
8.6 All actions taken will be recorded.
8.7 The Information Commissioners Office is to be notified in accordance with GDPR guidelines and requirements.

9.0 Evaluation and response

9.1 Once the initial incident is contained, the company will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.
9.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.
9.3 The review will consider:
9.3.1 Where and how personal data is held and where and how it is stored
9.3.2 Where the biggest risks lie, and will identify any further potential weak points within its existing measures
9.3.3 Whether methods of transmission are secure.
9.3.4 Identifying weak points within existing security measures Staff awareness
9.3.5 Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

9.4 If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by the company directors.