

Data protection policy

INTRODUCTION

GWE Business West are registered under the Data Protection Act 1998.

GWE Business West regard the lawful treatment of Personal Data as necessary for its successful operations, to maintain confidence between clients, partners, third partners and GWE Business West. It is GWE Business West policy to treat Personal Data lawfully by complying with the Data Protection Acts.

Accordingly, GWE Business West policy puts in place a process to allow clients to know what information is held, purposes for which it may be used and to have the opportunity to 'opt out' of having their data used for the given purposes. GWE Business West is committed to promoting compliance to Data Protection legislation and this policy and all GWE Business West staff are expected to comply with this policy.

The Data Protection policy also extends to personal information about employees and all GWE Business West staff are expected to comply with this policy.

APPLICABILITY

The policy is in relation to the following:

- All departments within GWE Business West
- Relationships with Partner organisations.
- Relationships with GWE Business West s' contractors; their employees and agents when providing services to:
 - GWE Business West
 - GWE Business West 's clients on behalf of GWE Business West.

Except to the extent that a GWE Business West department or affiliate is able to claim an exemption under relevant national legislation from any one or all of the Principles defined below in this policy, all of the Principles apply to all parties

This policy is applied to all contacts, regardless of the legal status of the client.

This policy applies to Personal Data whether in paper or electronic files, including archival copies wherever located.

This policy also applies to personal data for employees

GENERAL

This policy distinguishes between three aspects of responsibility for Data Protection compliance within GWE Business West.

- Managing the registration process and policy issues.
- Managing the client communication process and maintaining the client responses.
- Managing operations in compliance with Data Protection legislation and GWE Business West policy.

Each department or nominated group shall implement practices consistent with this policy statement.

RESPONSIBILITES

Registration, Process & Policy Issues

The Data Protection Working Group will be responsible for:

- Ensuring that the Data Protection policy reflects prevalent business needs.
- Ensuring that Data Protection registration is up to date, that the document is accurate and that relevant registration processes are adhered to.
- Monitoring external requests for data by partners and ensure that provision complies with access policy.
- This group will ensure that there are appropriate business processes in place to enable operational staff to comply with Data Protection legislation.
- This group will ensure that the IT infrastructure and database applications are in place to support Data Protection compliance.
- The group will include representation from the following functions: Information Services, IT, HR, Direct Marketing and Database management.

Client Data Protection Communications and Opt out process:

- Where possible, all communications, electronic or written, will hold a reference to the Web site or alternative contact point for access to the GWE Business West Privacy Statement, Data Protection policy and opportunity to 'opt out' of the specified uses or to request access to their personal data.
- All electronic direct mail will also offer the opportunity to opt out of any subsequent direct e-mail activities.
- Data Protection responses will be directed through the database office and will be recorded on the Client management System. A central file of responses is maintained.

Operations:

Service delivery Departments will do the following:

- Each department shall ensure that all working practices are compliant with Data Protection policy.
- Where a department requires hard copy Data Protection information and opt out at point of service delivery, it is the responsibility of the department to ensure compliance.
- Each department shall ensure that internal procedures are adjusted and maintained to reflect Data Protection policy
- Each department will ensure that internal IT applications comply with Data Protection policy
- Each department will ensure that internal manual data storage is compliant with Data Protection policy.
- Each department to ensure that field workers' and home workers' external data storage arrangements are compliant with Data Protection policy.
- Where a department passes data to a supplier for research or other legitimate purpose; the department must ensure that the supplier contract includes the Data Protection clause recognising GWE Business West ownership of the data; proscribing future or other use by the supplier.
- Where a department passes data to a third party contractor for the purpose of supplying service to a client; the department must ensure that the third party contractor's contract includes a Data Protection clause recognising GWE Business West ownership of the data; proscribing future or other use by the supplier
- Where a department organises an event or seminar where there will be a Delegate list; delegates must be given the opportunity to not appear on the list.

- Each department is responsible for implementing and administering this policy and the guidelines with immediate effect.

Marketing Department

- All direct mailings, electronic or postal, must exclude any contact who has opted out of receiving marketing communications.
- All direct mailings, electronic or postal, must screen for centrally held 'opt out' lists. Any transfer of information must exclude any contact that has opted out of data transfer.
- Any electronic direct mail must exclude any contact that has opted out of receiving electronic marketing.
- Any electronic direct mail must include the opportunity to opt out of subsequent electronic marketing contact
- Any telephone marketing must exclude any contact who has opted out of receiving telephone marketing contact, and any contact who has registered with the telephone preference service.
- All regular communication mailings must offer the opportunity to unsubscribe.

Definitions

For the purposes of this policy the following words have the following meanings:

Personal Data means any information relating to an identified or identifiable natural person.

Data Subject means an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his and her physical, physiological, mental, economic, cultural or social identity.

Exemptions means that under national or territorial law the Scope of the obligations and rights provided for in this policy are excluded or altered. Such exemptions may vary according to particular circumstance, nature of information and use.

Scope means that this policy applies to the Processing of Personal Data wholly or partly by automatic means, and to the Processing otherwise than by automatic means of Personal Data which form part of a filing system or are intended to form part of a filing system.

Principles means that Personal Data must be:

- Processed lawfully;
- Collected for specified, explicit and legitimate purposes and not further Processed in a way incompatible with those purposes;
- Not transferred to any other party except in compliance with Data Protection policy.
- Adequately protected, relevant and not excessive in relation to the purposes for which they are collected and/or further Processed;
- To the extent practicable, accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further Processed, are corrected;
- Kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further Processed. Where required by law, GWE Business West shall implement appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use;
- Processed in accordance with the rights granted by law to Data Subjects;

- Not transferred across national and/or territorial boundaries unless the country or territory to receive the Personal Data ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data; and
- Protected by appropriate technical and organizational measures against unauthorized or unlawful Processing and against accidental loss, destruction or damage.

Processing or Processed means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as: collecting; recording; organising; storing; adapting or altering; retrieving; consulting; using; disclosing by transmission; disseminating or otherwise making available; aligning or combining; blocking; erasing or destroying.

Third Party Data Processors means agents or contractors of GWE Business West providing services to GWE Business West that requires them to use GWE Business West personal data.

Penalties & Disciplinary Action

Any GWE Business West employee who knowingly violates or attempts to violate this Data Protection Policy or the Data Protection guidelines promulgated by a department or an affiliate of GWE Business West shall be subject to disciplinary action.

Any GWE Business West T employee who mistakenly violates the DP policy must inform the Data Controller immediately.

Under the Data Protection laws and regulations an employee of GWE Business West may be held to be individually responsible for compliance and may be personally liable to criminal or civil actions for breach of applicable Data protection laws or regulations.