gibsonwatts.

GDPR

Gibson Watts Policies

today's leaders, tomorrow's change

www.gibsonwatts.com

Gibson Watts needs to collect and use certain types of information about the Clients that we deliver services to, the candidates that we source roles for and the staff which we employ. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored on our server, collected by email or stored on phones, or recorded on other material and there are safeguards to ensure this under the General Data Protection Regulations

DATA CONTROLLER

Anne O'Donnell, CEO, is the Data Controller under the Regulations, which means that she determines what personal information held, will be used for. She is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

DISCLOSURE

Gibson Watts only share personal information pertaining to employees, clients and candidates with our Chartered Accountant and any Assessment Bodies appointed by our clients for the purpose of audits. Gibson Watts share Candidate Information with Clients and Client Information with Candidates only were authorised to do so by the relevant party. Gibson Watts will not share information with any other companies or agencies unless legally bound to do so.

If Information is shared for any reason, the Employee/Client/Candidate will be made aware in how and with whom their information will be shared. There are circumstances where the law allows Gibson Watts to disclose data (including sensitive data) without the data subject's consent.

These are:

a) Carrying out a legal duty or as authorised by the Secretary of State
b) Protecting vital interests of an Employee / Client / Candidate or other person
c) The Employee / Client / Candidate has already made the information public
d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights
e) Monitoring for equal opportunities purposes – i.e. race, disability or religion

f) Providing a confidential service where the Employee's / Client's / Candidate's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Employee's / Client's / Candidate's to provide consent signatures.

Gibson Watts considers the lawful and correct treatment of personal information as vital to successful working and maintaining the confidence of those with whom we deal.

We are committed to ensuring that all personal data is treated lawfully. To this end, out business will adhere to the Principles of Data Protection, as detailed in the General Data Protection Regulations.

Specifically, the Principles require that personal information:

a) Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
b) Shall be obtained only for one or more of the purposes specified in the Regulations, and shall not be processed in any manner incompatible with that purpose or those purposes,
c) Shall be adequate, relevant and not excessive in relation to those purpose(s)
d) Shall be accurate and, where necessary, kept up to date,
e) Shall not be kept for longer than is necessary
f) Shall be processed in accordance with the rights of data subjects under the Act,
g) Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
h) Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Employee's/Client's/Candidate's in relation to the processing of personal information.

Gibson Watts will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Ensure that the rights of people about whom information is held, can be fully exercised under the Regulations. These include:
    i. The right to be informed that processing is being undertaken,
    ii. The right of access to one's personal information
    iii. The right to prevent processing in certain circumstances and
    iv. GDPR Policy
    v. The right to correct, rectify, block or erase information which is regarded as wrong information)
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information

DATA COLLECTION

Data Collected by Gibson Watts in the most part is collected under the lawful basis of having a contract in place i.e. an employment contract is in place or an order has been placed to progress with works or a Candidate has asked us to source a role. Where a contract is not in place the lawful basis will be consent which is received in an appropriate manner as follows:

- An Employee / Client / Candidate clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data

- And then gives their consent.

Gibson Watts will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, our team will ensure that the Employee / Client / Candidate:

a) Clearly understands why the information is needed
b) Understands what it will be used for and what the consequences are should the Employee / Client / Candidate decide not to give consent to processing
c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
e) Has received sufficient information on why their data is needed and how it will be used

DATA STORAGE

Information and records relating to Clients and Candidates will be stored securely and will only be accessible to authorised staff. All data is stored within our Cloud Server system, which is a permission controlled, secure cloud system and is only accessible by those who have been assigned appropriate permissions.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is our responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

DATA STORAGE FOR THE PURPOSE OF RECRUITMENT

Information collected for the purpose of sourcing roles on behalf of Candidates or identifying Candidates for roles such as CV's, Job Descriptions, etc... will be held

for as long as it is required and once the commission has been completed the data will be deleted from our system within a period of 6 months.

DATA ACCESS AND ACCURACY

All Employees / Clients / Candidates have the right to access the information we retain about them. Our team will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

Gibson Watts will ensure that:

- It has a Data Controller with specific responsibility for ensuring compliance with Data Protection
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so
- Everyone processing personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information
- It will regularly review and audit the ways it hold, manage and use personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

RETENTION

Records should be kept for as long as they are needed to meet the operational needs of our business but no less than 7 years, together with legal and regulatory requirements. We have assessed our records to:

- determine their value as a source of information about Gibson Watts, its operations, relationships and environment,
- determine their value as a source of valuable information regarding clients/candidates, their conditions and treatments.
- assess their importance as evidence of business activities and decisions
- establish whether there are any legal or regulatory retention requirements (including: Public Records Act 1958, General Data Protection Regulations, the Freedom of Information Act 2000 and the Limitation Act 1980).

DISPOSAL

A disposal schedule is a key document in the management of records and information. It is a list of series or collections of records for which predetermined periods of retention have been agreed by the Data Controller.

Records on disposal schedules will be as follows:

Destroy after an agreed period – where predetermined as 7 years for all normal records the company holds, or a pre-determined time as defined by clients.

DESTRUCTION

- Non-sensitive information – can be placed in a normal rubbish bin
- Confidential information – cross cut shredded and pulped or burnt.
- Electronic equipment containing information - destroyed using killdisc and for individual folders, they will be permanently deleted from the system.

Destruction of electronic records should render them non-recoverable even using forensic data recovery techniques.

SHARING OF INFORMATION

Duplicate records should be destroyed. Where information has been regularly shared between business areas, only the original records should be retained in accordance with the guidelines detailed above. Care should be taken that seemingly duplicate records have not been annotated.

Where we share information with other bodies, we will ensure that they have adequate procedures for records to ensure that the information is managed in accordance with the relevant legislation and regulatory guidance.

DOCUMENT DELETION/DISPOSAL

A record / log of deletions and disposals must be maintained on Form GDPR/001.

This should include:

- the details of the record
- the type of record
- the retention period
- the reason for deletion / disposal
- the method of deletion / disposal
- the person responsible for the deletion / disposal

DATA BREACH

In the event of a data breach by loss of information whether in hard copy or electronic copy or a malware or ransomware virus on a company pc or server that removes data we will:

- Address the physical breach by shutting down systems and processes to ensure the data breach does not continue.
- Fully investigate the breach to determine why and how this happened and put in place measures to prevent the re-occurrence of the breach.
- Determine whether the information is high risk information or low risk information. High Risk information is determined as any information that can cause harm to an individual or business.
- If the breach is High Risk Information, then Gibson Watts will notify the ICO and the victim of the data breach (the person or company that the data pertains to) within 72 hours of the data breach.
- If the breach is low risk, then Gibson Watts will advise the victim of the data breach in writing within 14 days.

PERSONAL INFORMATION ON EMPLOYEES, CANDIDATES OR CLIENTS

Gibson Watts will provide all information pertaining to an employee, candidate or client to the employee, candidate or client that the information pertains to within one month of receipt of the request. This will either be provided in a hard copy format or emailed as a zip file.

Where employees, candidates or clients are no longer employees, candidates or clients of Gibson Watts we will provide information in the same manner as detailed above within one month.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulations. Where changes are made to the way we treat and manage data this will be communicated to all Employees, Clients and Candidates via email update


gibsonwatts®
todays leaders, tomorrow's change