Data Protection Policy

Contents

Contents

1. Introduction

In the course of everyday business Complete Business Solutions needs to gather and use certain information relating to individuals. These may include clients, suppliers, business contacts, employees and other people Complete Business Solutions has a relationship with or may need to contact.

This policy describes how this personal data is collected, processed and stored to meet Complete Business Solutions obligations under the General Data Protection Regulation (GDPR) which is effective from 25 May 2018.

Complete Business Solutions is committed to protecting the rights and freedoms of data subjects and securely and transparently processing their data in accordance with all legal obligations.

2. Purpose of this Policy

This policy sets out how Complete Business Solutions seeks to protect personal data and ensure all employees understand and adhere to the rules governing how they process personal data to which they have access in the course of their employment. Everyone who works for, on behalf of, or with Complete Business Solutions has responsibility for ensuring data is collected, stored and handled appropriately and in accordance with data protection principles.

3. Definitions

3.1 Business Purposes

The purposes for which personal data may be used by Complete Business Solutions: Personnel, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following:

- Compliance with our legal obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business policies are adhered to (such as policies covering e-mail and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Marketing our business
- Improving services.

3.2 Personal Data

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data we gather may include: individuals' home address, phone number, e-mail address, educational background, financial details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

3.3 Special Categories of Personal Data

Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences or related proceedings, and genetic and biometric information - any use of special categories of personal data should be strictly controlled in accordance with this policy.

3.4 Data Controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

3.5 Data Processor

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

3.6 Data Subject

The individual who the personal data relates to.

3.7 Processing

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.8 Supervisory Authority

The national body responsible for data protection. The supervisory authority for Complete Business Solutions is the Information Commissioners Office (ICO).

4. Data Protection Law

The General Data Protection Regulation (GDPR) is effective from 25 May 2018. This describes how organisations must collect, handle and store personal information. These rules apply to data stored electronically or in physical format.

5. Scope of this Policy

This policy applies to all employees and any person working on behalf of Complete Business Solutions who must read and understand the contents of the policy and how it applies to them. This includes external processors such as;
Trusted Bank's, Trusted Wholesalers, Trusted Carriers, Big Change Apps, ECi and trusted Service Providers, i.e. HP and Microsoft
This policy supplements Complete Business Solutions policies relating to internet and e-mail use. We may supplement or amend this policy by additional policies and guidelines from time to time.

6. Who is Responsible for this Policy

6.1 The Board / Company Directors

The Management Board have overall responsibility for ensuring that Complete Business Solutions meets its legal obligations and has day to day responsibility of this policy.

6.2 Data Protection Officer

- The Regional IT Managers are the appointed Data Protection Officer (DPO)
- Briefing the IT Director on Data Protection responsibilities such as employee and client data
- Reviewing Data Protection and related policies
- Advising on tricky Data Protection issues
- Ensuring that Data Protection induction and training takes place across the group and is in the employee contract
- Understand how to notify the ICO regarding breaches
- Handling subject access requests from employees and recording and escalation to the IT Director
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors.

6.3 Specific Department Heads

The Regional IT Managers will monitor themselves for IT compliance reporting back to the DPO. Marketing will monitor their own compliance and report back to the DPO.

6.4 Employees & Volunteers

All staff and volunteers should be required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (From now on, where 'employees' is used, this includes both paid employees and volunteers.)

6.5 Enforcement

The GDPR enforces a maximum of 4% fine or 20M Euro's for significant data breaches. Due to our employee contracts, internal emails are monitored. Should any personal information be disclosed and an employee has gone through their training, this may lead to dismissal.

7. General Guidelines for Employees

- Complete Business Solutions will provide training to all employees to help them understand their personal responsibilities when handling data.
- Data should only be accessed by those employees who need to do so for the purpose of carrying out their personal employment duties.
- Employees should keep all data as secure as possible by complying with our Data Storage and Security Policy.
- Data should not be disclosed to unauthorised recipients, either internally or externally.
- Data should be reviewed regularly and updated to ensure accuracy and relevance.
- Employees should seek assistance from the DPO if they are unsure about any aspect of data protection.

8. The Principles

Complete Business Solutions shall comply with the principles of data protection (the Principles) of the General Data Protection Regulation 2018 (GDPR). We will make every effort possible in everything we do to comply with these principles. The Principles are:

a) Lawful, fair and transparent
Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

b) Limited for its purpose
Data can only be collected for a specific purpose.

c) Data minimisation
Any data collected must be necessary and not excessive for its purpose.

d) Accurate
The data we hold must be accurate and kept up to date.

e) Retention
We cannot store data longer than necessary.

f) Integrity and confidentiality
The data we hold must be kept safe and secure.

g) Accountability and transparency
We must ensure accountability and transparency in all our use of personal data.

We must show how we comply with each Principle. We will be responsible for keeping a written record of how all the data processing activities we are responsible for comply with each of the Principles. This will be kept up to date and approved by the DPO.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we need to demonstrate compliance. All employees are responsible for understanding their responsibilities to ensure that we:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conduct Data Protection Impact Assessments where necessary
- Implement measures to ensure privacy by design and default, including data minimisation, pseudonymising, transparency, allowing individuals to monitor processing, and creating and improving security and enhanced privacy procedures on an ongoing basis.

8.1 Data Controlling and Data Processing

Complete Business Solutions is classified as a data controller and data processor. We must maintain our appropriate registration with the Information Commissioners Office (ICO) in order to continue lawfully controlling and/or processing data.

As a data processor, we must comply with our contractual obligations and act only on the documented instructions of the data controller. If we at any point determine the purpose and means of processing we shall be considered a data controller and therefore have the same liability as the controller. As a data processor, we will:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches.

If there is any doubt about how we handle data, please contact the DPO for clarification

8.2 Lawful Basis for Processing Data

We will always establish a lawful basis for processing all data. All employees must ensure that any data they are responsible for managing has a written lawful basis. It is the individual employee's responsibility to check the lawful basis for any data being worked on and ensure all actions comply with the lawful basis. At least one of the following conditions must apply whenever we process personal data:

a) Consent
We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

b) Contract
The processing is necessary to fulfil or prepare a contract for the individual.

c) Legal obligation
We have a legal obligation to process the data (excluding a contract).

d) Vital interests
Processing the data is necessary to protect a person's life or in a medical situation.

e) Public function
Processing is necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

f) Legitimate interest
The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

8.3 Deciding Which Condition to Rely On

If we make an assessment of the lawful basis, we must first establish that the processing is necessary. This means the processing must be an appropriate way of achieving the stated purpose. We cannot rely on a lawful basis if we can reasonably achieve the same purpose by some other means.

More than one basis may apply, and we should rely on what will best fit the purpose, not what is easiest.

In considering which condition to rely on we will look at the following factors and document our decision:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- Is the lawful basis we consider most appropriate the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are we in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are we able to stop the processing at any time on request and have we factored in how to do this?

Our commitment to the first Principle requires us to document this process, show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We will also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This is documented in our Privacy Notice (which is available on our website or upon request). This applies whether we have collected the data directly from the individual, or from another source.

9. Special Categories of Personal Data (formerly sensitive personal data)

This means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, and sexual orientation.

We process special categories of data in only very limited circumstances. However, where we process special categories of personal data we will obtain the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

If we do not have a lawful basis for processing special categories of data we will discontinue processing the relevant data immediately.

10. Responsibilities

Complete Business Solutions responsibilities include the following:

- Analysing and documenting the type of personal data we hold.
- Checking procedures to ensure they cover all the rights of the individual.
- Identifying and documenting the lawful basis for processing data.
- Ensuring consent procedures are lawful.
- Implementing and reviewing procedures to detect report and investigate personal data breaches.
- Storing data in safe and secure ways.
- Assessing the risk that could be posed to individual rights and freedoms should data be compromised.
- Reviewing all data protection procedures and policies on a regular basis.
- Arranging data protection training and ongoing advice for all employees.
- Responding appropriately and within the terms of our legal requirements to any subject access requests.
- Checking and approving third parties handling any data outsourced by Complete Business Solutions
- Ensuring (with the assistance of our IT support team) that all systems, services, software and equipment meet acceptable security standards.

Employee responsibilities include the following:

- Fully understanding their data protection obligations
- Checking that any data processing activities they are dealing with comply with our policy and are justified
- Not using data in any unlawful way
- Not storing data incorrectly, being careless with it or otherwise causing us to breach data protection laws and our policies through their actions
- Complying with this policy at all times
- Raising any concerns, notifying any breaches or errors, and reporting anything suspicious or contradictory to this policy or our legal obligations without delay.

10.1 Accuracy and Relevance of Data

We will always seek to ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should inform the DPO immediately.

10.2 Data Security

We will do everything we can to keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, we will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

10.3 Storing Data Securely

- Where personal data is stored manually (such as personnel records), it will be kept in a secure, locked cabinet where unauthorised personnel cannot access it.
- Printed data will be shredded as soon as it is no longer needed.
- Data stored on a computer will be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks should be encrypted or password protected and locked away securely when they are not being used.
- Servers are kept in a secure location, away from general office space.
- Data will be regularly backed up in line with the company's backup procedures.
- All reasonable technical measures are put in place to keep data secure.

10.4 Data Retention

We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our Privacy Policy.

10.5 Transferring Data Internationally

We will not transfer personal data abroad, or anywhere else outside of normal business rules and procedures without permission from the data subject.

11. Rights of individuals

Individuals have rights to their data which we will always respect and comply with to the best of our ability. We will ensure individuals can exercise their rights in the following ways:

a) Right to be informed

- We will provide Privacy Notices which are concise, transparent, intelligible and easily accessible, free of charge, written in clear and plain language.
- We will keep a record of how we use personal data to demonstrate accountability and transparency.

b) Right of access

- Enabling individuals to access their personal data and supplementary information.
- Allowing individuals to be aware of and verify the lawfulness of the processing activities.

c) Right to rectification

- Upon request, we will rectify the personal data of the individual because it is inaccurate or incomplete.
- This will be done without delay and no later than one month. This can be extended to two months in certain circumstances, but this must be agreed by the DPO and the individual notified.

d) Right to erasure

- We will delete or remove an individual's data if requested and there is no compelling reason for its continued processing (e.g. we need to retain information for the defence of a legal claim).
- If personal data has been passed on to other parties or recipients, we will contact those recipients and inform them of their obligation to erase the data. We will seek written confirmation of their compliance with the request.

e) Right to restrict processing

- We will comply with any reasonable request to restrict, block, or otherwise suppress the processing of personal data.

f) Right to data portability

- We will provide individuals with their data in a commonly used, machine-readable format, and send it directly to another controller if requested.

g) Right to object

- Individuals have the right to object to their data being used. Upon request we will cease processing unless we have legitimate grounds for processing which override the interests, rights and freedoms of the individual or the processing relates to the establishment, exercise or defence of legal claims.
- We will always inform the individual of their right to object at the first point of communication, i.e. in the Privacy Policy which is available upon request.

h) Rights in relation to automated profiling and decision making

- It is Complete Business Solutions policy not to use automated decision making and profiling.

12. Privacy Policy

Our Privacy Policy is available on our website or upon request from GDPR@complete.co.uk

13. Subject Access Requests

We will provide access to personal data in all reasonable circumstances (subject to sufficient proof of entitlement) and will notify those making access requests of the purpose of the processing, the type of data held, who the data has been or will be disclosed to, and the period for which the data will be stored. Individuals making successful subject access requests can request rectification or erasure of personal data, restriction of processing of personal data concerning the data subject, or to object to such processing.

13.1 How Complete Business Solutions handles Subject Access Requests

We will provide an individual with a copy of the information requested, free of charge, in commonly used electronic format (e.g. PDF or Word documents) within one month of receipt of a reasonable written request.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we may request the individual specify the information they are requesting.

A copy of Complete Business Solutions Subject Access Request template is available upon request from GDPR@complete.co.uk

14. Third parties

As a data controller and data processor, we have written contracts in place with any third-party data controllers and data processors that we use.

As a data controller, we will only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected at all times.

As a data processor, we will only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects at all times.

14.1 Data Audits

We will carry out regular data audits to manage and mitigate risks. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

14.2 Monitoring

Everyone must observe and comply with this this policy. The DPO has overall responsibility for this policy. Complete Business Solutions will keep this policy under review and amend or change it as required. Any breaches of this policy must be notified to the DPO immediately.

14.3 Staff Training

All employees will receive adequate training on provisions of data protection law specific for their individual role. All training must be completed as requested. If any employee requires additional training on data protection matters, they should contact the DPO.

14.4 Reporting Breaches

Any breach of this policy or of data protection laws must be reported as soon as is practically possible. This means as soon as someone becomes aware of a breach. Complete Business Solutions has a legal obligation to report any serious data breaches to the ICO within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures. These must be elevated to the GDPR team who will investigate and contact the ICO where necessary. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material.

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures, will be liable to disciplinary action.

14.5 Non-compliance

Complete Business Solutions are fully committed to protecting individuals' data rights. Failure of any employees of Complete Business Solutions to comply with any requirement of this policy may lead to disciplinary action and possible dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the GDPR team, Complete Business Solutions, Unit 4 Daughters Court, Silkwood Park, Ossett, Wakefield WF5 9TQ or email GDPR@complete.co.uk

14.6 Complaints

You have the right to lodge a complaint with the ICO in respect of any aspect of data protection, if you feel that we have not complied with the requirements of GDPR – www.ico.org.uk.

15. References

Privacy Policy – this document sets out Complete Business Solutions policy and procedures for processing personal data through our website, mobile applications and online services.

Access Control Policy – this document sets out Complete Business Solutions policy and procedures for the control of electronic documents and data.

Information Security Policy – this document sets out Complete Business Solutions procedures for the use of computer and other systems and requirements for information security.

Employees' Handbook – the handbook contains further information relating to the processing of personal information.

Leigh Everington
Managing Director