GENERAL DATA PROTECTION POLICY

AUTHOR	Kevin Davies
DATE	27 February 2018
VERSION	3.0
STATUS	Release

1 TABLE OF CONTENTS

2 INTRODUCTION

Aspin (“we”) hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that customers and staff understand the rules governing their use of personal.

This policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

2.1 Business purposes

The purposes for which personal data may be used by us:

Personnel, administrative, financial, regulatory, payroll, service operation and business development purposes.

Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance 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 email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information and security vetting
- 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
- Delivering, supporting and improving services

2.2 Personal data

Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, reps, suppliers, prospects and marketing contacts.

Personal data we gather may include: individuals' contact details, rep location, user ID, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, visa application status and CV.

2.3 Sensitive personal data

Personal data 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 — any use of sensitive personal data is strictly controlled in accordance with this policy.

We do not collect or store any sensitive personal data relating to customers, prospects, or our customers' customers.

2.4 Scope

This policy applies to all employees who are required to be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

2.5 Who is responsible for this policy?

As our Data Protection Officer, Kevin Davies has overall responsibility for the day-to-day implementation of this policy.

3 OUR PROCEDURES

3.1 Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

3.2 The Data Protection Officer's Responsibilities:

- Keeping the directors and senior management updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by Aspin Management Systems Ltd.
- Checking and approving third parties that handle the company's data and any contracts or agreements regarding data processing

3.3 Responsibilities of the IT Manager

- Ensuring all systems, services, software and equipment meet acceptable security standards (based on vendor recommendations and best practice)
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services, the company is considering using to store or process data

3.4 Responsibilities of the Company Secretary

- Updating sensitive/private employee information to ensure that is accurate
- Addressing data protection queries from employees
- Coordinating with the DPO to ensure all employee data adheres to data protection laws and the company's Data Protection Policy
- Responsibilities of the Marketing Manager
- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets

- Coordinating with the DPO to ensure all customer data, prospect data and marketing initiatives adhere to data protection laws and the company's Data Protection Policy

3.5 The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our Terms of Business contains a Privacy Notice to clients on data protection.

The notice:

- Sets out the purposes for which we hold personal data on customers and employees
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that customers have a right of access to the personal data that we hold about them

3.6 Sensitive personal data

In cases where we process sensitive personal data we will require 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.

3.7 Accuracy and relevance

We will 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 record the fact that the accuracy of the information is disputed and inform the DPO, Kevin Davies.

3.8 Personal data

Individuals must take reasonable steps to ensure that personal data we hold is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer or Company Secretary so that they can update our records.

3.9 Data security

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

3.10 Storing data securely

- In cases when data is stored on printed paper, we will ensure it is kept in a secure place where unauthorised personnel cannot access it
- Printed data will be shredded when it is no longer needed
- Data stored on a computer will be protected by encrypted disks/filesystems (where possible) and strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Any backup tapes are locked away securely when they are not being used
- The DPO must approve any cloud providers used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly and securely backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones (unless required for the processing of that data). In cases where it is required, the device will use an encrypted filesystem and strong passwords where possible
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

3.11 Data retention

We must 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 data retention guidelines.

3.12 Transferring data from site to site

All data will be transferred using secure protocols: HTTPS (SSL/TLS), SSH etc. using the most secure protocols available.

3.13 Transferring data internationally

There are restrictions on international transfers of personal data. Our normal business practice does not require us to transfer personal data out of the UK. If special circumstances arise where we need to transfer data outside the UK, we will not do so without first consulting the DPO.

4 SUBJECT ACCESS REQUESTS

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.

Anyone receiving a subject access request should refer that request immediately to the DPO.

Please contact the DPO if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

4.1 Processing data in accordance with the individual's rights

We will abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

We will not send direct marketing material to someone electronically (e.g. via email) unless we have an existing business relationship with them in relation to the services being marketed.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

4.2 Training

All staff will receive training on this policy. New joiners will receive training as part of their induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house training session.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory. Employee attendance and acceptance are recorded.

5 GDPR PROVISIONS

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

5.1 Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation.

We are happy to provide details about how we collect data and what we will do with it on a per-product basis (for customers) and on an individual basis (for employees, contractors, prospective employees, etc.).

Customers can refer to our product-specific personal data tables for more information on individual products.

If you have not been sent details for the products and services we provide your organisation, please contact our support team by email at support@aspin.co.uk or by phone on 01794 500 200 and they will be happy to provide them to you.

5.2 Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

5.3 Justification for personal data

We will process personal data in compliance with all six data protection principles

We will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

5.4 Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

5.5 Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

5.6 Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

5.7 Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

5.8 Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

5.9 International data transfers

No data may be transferred outside of the EEA without first discussing it with the data protection officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

5.10 Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. 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.

5.11 Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Any actual or potential data protection compliance failures should be reported to the DPO.

5.12 Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy and will monitor it regularly to make sure it is being adhered to.

6 CONSEQUENCES OF FAILING TO COMPLY

We take compliance with this policy very seriously. Failure to comply puts both the organisation and our customers at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.