VA Services

Data Protection Policy

Version	Date	Author	Rationale
V0.1	Oct 2020	Leanne Pogson Leap HR	First Draft
V0.2	Dec 2020	Emma Morris Find My Unicorn	Final Review
V0.3	Feb 2021	Emma Morris Unicorn VA Services	Change of business name and logo

Introduction

We hold personal data about our 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 all involved understand the rules governing their use of personal data to which they have access in the course of their work. This policy requires us 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.

Definitions

Business Purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll 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, security vetting, credit scoring and checking • 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
Personal Data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers, and marketing contacts. Personal data we gather may include individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV
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 should be strictly controlled in accordance with this policy.

Scope

This policy applies to all staff. You must 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.

Who is responsible for this policy?

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

Our procedures

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.

The Data Protection Officer's responsibilities:

- Keeping the board 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 Unicorn VA Services
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Responsibilities of the IT Manager

- Ensure all systems, services, software, and equipment meet acceptable security standards
- 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

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 marketing initiatives adhere to data protection laws and the company's Data Protection Policy

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

Sensitive personal data

In most 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.

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, Emma Morris.

Your personal data

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

Data security

You must 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.

Storing data securely

- We do not store any data on printed paper
- Data stored electronically is protected in the following ways

    - All passwords are encrypted and only accessed through LastPass
    - All data is stored via Cloud storage using Microsoft 365 Business Premium and only accessed via 2-step authentication
    - All hardware is backed up to an external drive weekly and stored securely
- We do not store data on CDs or memory sticks
- The DPO approves any cloud used to store data
- We do not store data directly to mobile devices such as laptops, tablets, or smartphones

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data internationally

There are restrictions on international transfers of personal data. We would not transfer personal data anywhere outside the UK without first consulting the Data Protection Officer and the data subject.

Subject access requests

Please note that under the Data Protection Act 2018, individuals are entitled, subject to certain exceptions, to request access to information held about them.

Please contact the Data Protection Officer, Emma Morris (contact details at the end of this policy) to make an access request.

Responses to subject access requests will be given within one (1) month and the data subject can expect to receive the following information:

- what we are using your information for
- who we are sharing your information with
- how long we will store your information, and how we made this decision
- details on your rights to challenge the accuracy of your information, to have it deleted, or to object to its use
- your right to complain to the IC
- details about where we got your information from

- whether we use your information for profiling or automated decision-making and how we are doing this; and
- what security measures we took if we have transferred your information to a third party

Processing data in accordance with the individual's rights

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

GDPR provisions

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

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. The following are details on how we collect data and what we will do with it:

What information is being collected?	**Client Information** – Contact name, contact phone numbers, contact email addresses, company name, company address, company website, required website addresses required to carry out work, passwords required to carry out work (we highly recommend all clients set up a free LastPass account and securely share passwords through this, if clients choose to share passwords directly, these are then stored securely in LastPass) **Other Data** – contact name, contact email addresses, company name, company website
Who is collecting it?	Data Protection Officer, Emma Morris
How is it collected?	Via Client Onboarding Documentation, email, newsletter opt in form,
Why is it being collected?	To ensure we can efficiently carry out the required work and to build an effective and up to date email marketing list

How will it be used?	To ensure we can efficiently carry out the required work, to communicate with the client and to issue invoices, to communicate with data subjects that have agreed to receive email marketing
Who will it be shared with?	No third parties
Identity and contact details of any data controllers	Emma Morris, emma@findmyunicorn.co.uk
Details of transfers to third parties	N/A
Retention period	For the duration of a client contract or until the data subject asks for information to be removed, whichever is first

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.

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.

Consent

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

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.

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.

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.

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.

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.

Reporting breaches

All actual or potential data protection compliance failures will be:

- Investigated to establish the failure and take remedial steps if necessary
- Maintained on a register of compliance failures
- Notified to the Supervisory Authority (SA) of any compliance failures that are material either or as part of a pattern of failures

Monitoring

The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

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