Versalift UK Limited

GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

GENERAL DATA PROTECTION REGULATION

This policy sets out how Versalift Distributors (UK) Limited's (hereafter referred to as "the Company" or "we"), will seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access to in the course of their work. In particular, 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.

The Company take the privacy of its employee, customers and suppliers very seriously.

This policy will be enforceable as of 25th May 2018.

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 individuals' racial or ethnic background, political opinions, religious or similar beliefs,*

trade union membership (or non-membership), physical or mental health condition, criminal offences, or related proceedings – any use of sensitive personal data should be strictly controlled in accordance with this policy and explicit consent obtained.

Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms.

This policy supplements all our other policies relating to the internet and email use. We may supplement and 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?

The Company's Data Protection Officer (DPO), 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 Versalift (UK) Limited*
- *Checking and approving with third parties that handle the Company's data any contract or agreement regarding data processing*

Responsibilities of the IT Manager

- *Ensures 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 or using to store or process data*

Responsibilities of the Marketing Manager

- *Approving data protection statements attached to emails and other marketing documentation*
- *Addressing data protection queries from clients, target audiences and/or media outlets*
- *Co-ordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the Company's GDPR 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 purpose 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 and if found to be incorrect, will be corrected as soon as is reasonably practicable (in most circumstances without undue delay). This includes any requests for data to be deleted/removed from our databases

Sensitive Personal Data

In most cases where we process sensitive personal data we will require the data subjects 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 the information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Data Protection Officer, Coral Headley.

Your Personal Data

You must take reasonable steps to ensure 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

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage staff to use a password manager to create and store their passwords
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The DPO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall

Data Retention

We must retain data for no longer than is necessary. What is necessary will depend upon the circumstances of each case, taking in to account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines *(see appendix I).*

Transferring Data Internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside of the UK without first consulting the Data Protection Officer.

Subject Access Requests (SAR)

Please note that under the General Data Protection Regulation individuals are entitled to request information held about them.

We ask that you make such request in writing to the Data Protection Officer, there is no charge for this request. However, if a request is manifestly unfounded or requests become excessive the Company may charge a fee for this service.

If your request is made electronically (e.g. by email). Where a request is made electronically, the information will be provided in a commonly-used electronic form, unless otherwise requested by the individual.

Your request will allow you to know what information is being held about you and what processing is carried out.

You should allow and expect a response within one month from the date of request.

In certain circumstances the Company may withhold personal data if by disclosing it would adversely affect the rights and freedom of others and/or disclose trade secrets.

Processing Data in Accordance with the Individual's Rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO of any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you 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.

Training

Training is provided through in-house training course, policy issue and/or tool box talk.

It will cover:

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

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.

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 will be available in the form of a privacy or fair processing notice.

1. **Consent –** the individual has given clear consent to process their personal data for a specific purpose.
2. **Contract –** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. **Legal Obligation –** the processing is necessary for you to comply with the law (not including contractual obligations)'

4. **Vital Interests –** the processing is necessary to protect someone's life.
5. **Public Task –** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. **Legitimate Interests –** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Justification for Personal Data

We will process personal data in compliance with the data protection principles, as detailed below:

1 **Lawful, fair and transparent**	2 **Limited for its purpose**	3 **Adequate and necessary**
4 **Accurate and up to date**	5 **Not kept for longer than necessary**	6 **Integrity and confidentiality**
7 **Personal information must be secure**	8 **Personal information not transferred to other countries without adequate protection**	

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

Consent

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

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.

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. There is no charge for this request.

Right to be Forgotten

A data subject may request that any information held on then 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. When relevant, and where 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. Where data is to be transferred outside of the EEA, the Company will ensure the recipient has Adequacy Status or Privacy Shield.

Data Audit and Register

Regular audits to manage and mitigate risks. The register 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 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 and all breaches whether or not they result in a notification to the Supervisory Authority
- Notify the Supervisory Authority of any compliance failures that are material either in their own right or as a pattern of failures

Please refer to the Company's Notification of a Personal Data Breach Policy for full details of our reporting procedure.

Monitoring

Everyone is responsible to observe this policy. The Data Protection Officer has overall responsibility for this policy. The policy will be monitored regularly to ensure it is being adhered to.

Consequences of Failing to Comply

We take compliance of this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our disciplinary procedures up to and including dismissal.

Review date: Annually or in line with any changes in "The Regulation", whichever comes first.

Appendix I – RETENTION OF PERSONAL DATA GUIDELINES

Recruitment

All CV's and correspondence hard copy and electronic will be destroyed 6 months after the date of the commencement of the recruitment campaign.

Where an unsolicited CV has been received by the Company. This will be destroyed 6 months from date of receipt, unless this pertinent to a recruitment campaign currently running at the time of receipt. In that case it will be destroyed in line with the above retention guideline of 6 months.

Ex-employee's

Any leaver of Versalift (UK) Limited, personnel hard copy file will be kept for a period of 6 years and consequently destroyed 6 years from the date of leaving.

Any data kept on the Company's payroll and/or HR systems will also be deleted in line with the above retention guideline of 6 years. Except bank details, pension and HMRC data, this will be destroyed and deleted from the Company's payroll and/or HR systems 3 years from date of leaving.

Any leaver can explicitly request in writing to have their data destroyed and deleted. However, pension and HMRC data must be kept for a period of 3 years in line with our legal obligations. In this case we will be unable to provide a reference for future employers. A hard copy reference detailing, length of service, job title and reason for leaving can be provided prior to leaving upon request.

Customers (Sales and Marketing)

Data relating to customers of Versalift (UK) Limited that no longer have a business relationship with us. Their data will be destroyed 6 years from the termination of the business relationship or last sale, whichever is latest. Unless explicit consent is received from the customer to retain their personal data for future marketing information.

Suppliers (Purchasing)

Data relating to suppliers to Versalift (UK) Limited that no longer have a business relationship with us. Their data will be destroyed 6 years from the termination of the business relationship or last sale, whichever is latest. Unless explicit consent is received from the supplier to retain their personal data.