

Privacy Policy

September 2020



VolkerWessels UK Privacy Policy

Issue 2, September 2020

1. PURPOSE

VolkerWessels UK is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the company commitment to data protection, and individual rights and obligations in relation to personal data.

It is essential that any employee, worker or contactor who is involved in any aspect of processing, managing or analysing personal data is aware of this document and adheres to the requirements contained within it. Ultimately, it is the responsibility of the senior management within VolkerWessels UK, including Heads of Departments, in conjunction with HR and the DPO, to ensure GDPR compliance.

VolkerWessels UK has appointed Jenny Scott-Russell, Legal Director for VolkerWessels UK as its Data Protection Officer. (DPO) The role of the DPO is to inform and advise VolkerWessels UK regarding its data protection obligations. The DPO can be contacted via the General Data Protection Regulation (GDPR) mailbox. The email address is gdpr@volkerwessels.co.uk if there are any questions about this policy or requests for further information, should be directed to the mailbox.

2. SCOPE

This policy applies to the personal data of job applicants, employees, workers, contractors, work experience and former employees, referred to as personal data. This policy does not apply to the personal data of clients or other data processed for business purposes.

3. DEFINITIONS

Personal data - is any information that relates to a living individual who can be identified from that information.

Processing - is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Special categories of personal data - means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sexual orientation and genetic and biometric data.

Criminal records data - means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

4. DATA PRIVACY POLICY

4.1 Principles

VolkerWessels UK processes personal data in accordance with the following data protection principles:

- Processes personal data lawfully, fairly and in a transparent manner.
- Collects personal data only for specified, explicit and legitimate purposes.
- Processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted immediately.
- Keeps personal data only for the period necessary for processing.
- Adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Approved for IMS:	IMS Manager	Document owner:	Legal Director	Workspace file:	n/a	Page 2 of 5
-------------------	-------------	-----------------	----------------	-----------------	-----	-------------

4. DATA PRIVACY POLICY (CONTINUED)

4.2 Communication

VolkerWessels UK informs individuals about the reasons for processing their personal data, how it uses such data and the legal basis for processing within *VolkerWessels UK Privacy Notice*. It will not process personal data of individuals for any other reasons. Where VolkerWessels UK relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that business interests are not overridden by the rights and freedoms of individuals.

Where VolkerWessels UK processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is implemented in accordance with GDPR regulations regarding special categories of data and criminal records data.

4.3 Data Storage

VolkerWessels UK will update personal data promptly if an individual advises that his / her information has changed or is inaccurate.

Personal data gathered during the employment, worker assignment, contractor assignment or work experience placement is held in the individual's personal file and on HR systems.

4.4 Data Retention

VolkerWessels UK will only retain personal information for as long as is necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for which we process personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances, we may anonymise personal information so that it can no longer be associated with an individual, in which case we may use such information without further notice to the individual. Once an individual is no longer an employee, worker or contractor of the company, we will retain and securely destroy the individual's personal information in accordance with applicable laws and regulations.

VolkerWessels UK keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the GDPR. Please refer to J03 *Personal Data Storage, Retention and Erasure* for further information.

4.5 Individual Rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject Access Requests

Individuals have the right to make a Subject Access Request (SAR). If an individual makes a SAR, VolkerWessels UK can tell him / her:

- Whether or not his / her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- To whom his / her data is or may be disclosed to, including recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- How long a SAR will usually take to be processed;
- His / her rights to rectification or erasure of data, or to restrict or object to processing;
- His / her right to complain to the Information Commissioner's Office if he / she thinks VolkerWessels UK has failed to comply with his / her data protection rights; and
- Whether or not VolkerWessels UK carries out automated decision-making and the logic involved in any such decision making.

VolkerWessels UK will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he / she agrees otherwise.

4. DATA PRIVACY POLICY (CONTINUED)

4.5 Individual Rights (Continued)

VolkerWessels UK will respond to a request within a period of one calendar month from the date it is received, unless the request is complex or numerous in which case the period can be extended by a further two months. In such a case, the individual will be notified within one month of making the request explaining why the extension is necessary.

Other Rights

Individuals have a number of other rights in relation to their personal data. They can require VolkerWessels UK to:

- Rectify inaccurate data;
- Stop processing or erase data that is no longer necessary for the purposes of processing;
- Stop processing or erase data if the individual's interests override VolkerWessels UK's legitimate grounds for processing data (where VolkerWessels UK relies on its legitimate interests as a reason for processing data);
- Stop processing or erase data if processing is unlawful; and
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override VolkerWessels UK's legitimate grounds for processing data.

To ask VolkerWessels UK to take any of these steps, the individual should send the request to gdpr@volkerwessels.co.uk

Data Security

VolkerWessels UK takes the security of HR related personal data seriously. The Company has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Details of which are included in *VolkerWessels UK Information and Communications Technology Policy*.

Where VolkerWessels UK engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of the data.

Impact Assessments

Some of the processing that VolkerWessels UK carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, VolkerWessels UK will carry out a Data Protection Impact Assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data Breaches

If VolkerWessels UK discovers that there has been a breach of HR related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. VolkerWessels UK will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken. Please refer to J01 *Data Breach Procedure* for further information.

International Data Transfers

VolkerWessels UK will not normally transfer HR-related personal data to countries outside the EEA. If such a transfer is planned, this will only be on the basis that, that country is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards by way of binding corporate rules or standard data protection clauses as necessary.

Approved for IMS:	IMS Manager	Document owner:	Legal Director	Workspace file:	n/a	Page 4 of 5
-------------------	-------------	-----------------	----------------	-----------------	-----	-------------

4. DATA PRIVACY POLICY (CONTINUED)

4.6 Individual Responsibilities

Individuals are responsible for helping VolkerWessels UK keep their personal data up to date. Individuals should let VolkerWessels UK know if data provided to the Company changes, for example, if an individual moves house or changes his / her bank details. Please refer to J03 *Personal Data Storage, Retention and Erasure* for further information.

Individuals may have access to the personal data of other individuals and of our clients in the course of their employment, assignment, work experience placement or apprenticeship. Where this is the case, VolkerWessels UK relies on individuals to help meet its data privacy protection obligations to staff and clients.

Individuals who have access to personal data are required:

- To access only data that they have authority to access and only for authorised purposes;
- Not to disclose data except to individuals (whether inside or outside VolkerWessels UK) who have appropriate authorisation;
- To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- Not to remove personal data, or devices containing or that can be used to access personal data, from VolkerWessels UK's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- Not to store personal data on local drives or on personal devices that are used for work purposes; and
- To report data breaches of which they become aware to the Data Protection Officer immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under *VolkerWessels UK Disciplinary Policy*. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

VolkerWessels UK will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them

5 IMS AUTHORISATION

Document owner approval:

Jenny Scott-Russell, Legal Director - 09.09.2020

Approval for IMS:

Andria Georgiou, IMS Coordinator - 11.09.2020

Approved for IMS:	IMS Manager	Document owner:	Legal Director	Workspace file:	n/a	Page 5 of 5
-------------------	-------------	-----------------	----------------	-----------------	-----	-------------