Vandura Ltd – Data Protection Policy

VANDURA
SOFTWARE. SIMPLIFIED.

This policy is written in accordance with the Data Protection Act 2018 and the General Data Protection Regulations 2018

Introduction

Vandura Ltd needs to gather and use some personal data about individuals and for their customers to use their product(s): Verifleet. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law. Vandura's data protection policy is published on its website and advises customers, employees and others what the data is being used for, how long it is kept and who it will be shared with.

What this policy covers

- This data protection policy ensures Vandura Ltd:

    - Complies with The Data Protection Act 2018 and GDPR Regulations 2018 and follows good practise
    - Protects the rights of employees and customers
    - Details how it stores and processes individuals' data
    - Protects itself from any data breach

Data Protection

The Data Protection Act 2018 and the GDPR Regulations of 2018 describes how organisations, like Vandura Ltd, must collect, handle and store personal information. These rules apply regardless of how data is stored.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

People

This policy applies to:

- The head office of Vandura Ltd

- Vandura Ltd employees

The information gathered, can include:

- Names of individuals
- Date of birth
- Postal addresses
- Email addresses
- Telephone Numbers
- The data to be gathered and shared may include vehicle registration numbers, names, and email addresses of drivers associated with vehicles, as well as the name of the client(s). This data is classified as sensitive information and will be protected accordingly.

Data Risks

This policy helps to protect Vandura Ltd from data security risks including:

- Breaches of confidentiality e.g. information given out inappropriately
- Failing to offer choice e.g. all individuals should be free to choose how the company uses data relating to them
- Reputational damage e.g. the company could suffer if hackers successfully gained access to sensitive data

Responsibilities

Everyone who works for or with Vandura Ltd has responsibility for ensuring that data is collected, stored and handled appropriately.

Every individual that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. These people have key areas of responsibility:

Head of Compliance

- Keeping the Vandura Ltd Board up-to-date about data protection responsibilities, risks and issues
- Reviewing all data stored, how data is handled, data protection procedures and related policies in line with an agreed schedule
- Arranging data protection training and advice for anyone covered by this policy
- Handling data protection questions
- Dealing with any subject access requests
- Checking any data shared with third parties that may handle sensitive data

Software Development Team

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks to ensure software is appropriate and the right security is in place
- To detect, report and investigate a personal data breach if required
- Continuously evaluating third party services used to store or process data e.g. cloud computing services

Vandura Ltd employees

The only people able to access data covered by this policy are those who need it for their work. Data must not be shared informally. Vandura Ltd will provide training to all employees to help them understand their responsibilities when handling data and employees must keep all data secure by taking sensible precautions.

Data Storage and Handling

Data provided by customers will be encrypted both during transfer and at rest in Google Cloud Platform (GCP) Cloud SQL (Postgres) and stored in the UK. Vandura's services are hosted in Google Kubernetes Engine (GKE) within the UK. Files, such as profile images and insurance documents, are secured in GCP Cloud Storage. Vandura's application is protected with Google's identity platform, ensuring no access to passwords. Google Secret Management is used for secure handling of API keys.

Additionally, anonymous MOT advisory details and contents of insurance policy documents (which may contain personal information) are shared with OpenAI's Chat

API. The OpenAI API used by Vandura Ltd and the Verifleet product is hosted in the UK by Microsoft Azure. OpenAI encrypts data at rest and retains it for 30 days solely for abuse monitoring purposes. OpenAI does not use this data for model training. For further information, please refer to OpenAI's Europe Terms of Use (https://openai.com/policies/terms-of-use/), Business Terms (https://openai.com/policies/business-terms/), and Enterprise Privacy (https://openai.com/enterprise-privacy/).

Data Retention

Customers may request deletion of their data at any time, and Vandura Ltd will comply with such requests promptly. We will only use and store information for so long as it is required for the purposes it was collected for and whilst they are a customer using Verifleet.

Data Accuracy

The law requires Vandura Ltd to take reasonable steps to ensure data is kept accurately and up to date.

Employees who work with data must ensure that it is:

- Retained accurately and is as up to date as possible
- Take every opportunity to ensure data is updated
- Vandura Ltd makes it easy for data subjects to update the information that the company holds about them by using Verifleet
- Data is updated or deleted by Verifleet users/ Vandura Ltd employees as inaccuracies are discovered

Subject Access Requests

Vandura Ltd aims to ensure that individuals are aware that their data is being processed and that they understand how the data is being used and how to exercise their rights. All individuals who are the subject of personal data held by Vandura Ltd are entitled to:

- Ask what information the company holds about them and why.
- Information held on an individual is readily available on Verifleet.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual or company contacts Vandura Ltd requesting this information this is called a subject access request. Subject access requests from individuals should be made by email and addressed to the Head of Compliance who will carry out the following procedure:

- The Head of Compliance will request the individual to complete a standard request form
- The Head of Compliance will provide the relevant data to the individual or company within one month
- The Head of Compliance will verify the identity of anyone making a subject access request before handing over information

Disclosing data for other reasons

In certain circumstances the Data Protection Act 2018 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances Vandura Ltd will disclose requested data after ensuring that the request is legitimate and seeking assistance from the Board of Directors and from the company's legal advisers where necessary.