DATA PROTECTION POLICY

PURPOSE

Veezu Holdings Limited ("Veezu") is committed to being transparent about how we collect, process, and retain personal data to meet our data protection obligations.

This policy sets out our commitment as well as the legal conditions that must be satisfied in relation to obtaining, handling, processing, storing, transporting, and destruction of personal information.

SCOPE

Our policy applies to all personal data collected, controlled, and processed by Veezu and its subsidiaries.

- Veezu North Limited (t/a Amber Cars and Britannia Radio Cars)
- Veezu Limited
- Veezu Assist Limited (also t/a Veezu.Insure)
- Veezu Midlands Limited
- Veezu Services Limited (also t/a Veezu.Partners)
- Panther Cambridge Limited (t/a Panther Taxis)
- Panther IP Limited
- A.B.C Taxis (EA) Limited (t/a ABC 666333, ABC Taxis, ABC Taxis Norwich)
- Northern Taxis Limited (t/a Veezu)
- Steel City Holdings Limited (t/a City Grab)
- Derby City Cars Limited
- City Taxis Holdings Limited

OUR RESPONSIBILITY

Veezu Compliance is responsible for the implementation and adherence to data protection regulations, including responsibility for maintaining policies and procedures that ensure personal data is adequately protected.

Veezu IT & Technical is responsible for the security of personal data in accordance with BS EN ISO/IEC 27001 2013.

COLLEAGUE RESPONSIBILITY

You must ensure that any personal information provided in connection with your employment is accurate and up to date. For example, you must notify Veezu People of any change to name, address, telephone number, bank details and/ or marital status as soon as possible.

You should complete and submit to people@veezu.co.uk, VEE033 Personal Details Form which is available to view and download from Veezu.Net.

You may be periodically asked to confirm any personal data held and are expected to comply with such requests.

You have access to the personal data of other individuals, driver partners and passengers and are responsible for meeting data protection obligations.

You are required to:

- Access data only when you have authority to do so and only for authorised purposes;
- Not disclose data except to individuals who have appropriate authorisation;

- 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 remove personal data, or devices containing, or that can be used to access personal data, from the workplace without consent from Veezu IT & Technical and your line manager. Appropriate security measures must be applied (such as encryption or password protection) to secure the data and the device;
- Not store personal data on local drives or on personal devices; and
- Report suspected data breaches in line with POL048 Data Breach Policy and Procedure, by submitting VEE122 Data Breach Reporting Form, which is available to view and download from Veezu.Net, to compliance@veezu.co.uk immediately

There are organisations or individuals, such as local authorities, Police, HMRC, or other statutory bodies with specific legal responsibilities who can require personal information to be released and which we are legally required to provide. However, before we lawfully disclose any information held, confirmation is required that the person requesting it is legally able to do so.

All requests for personal information should be made in writing, providing precise details of the authority/body asking for the information and the legal basis for us to supply the information. VEE054 Request for Disclosure Form is available via the Veezu.Net for this purpose.

There are also circumstances where other organisations such as solicitors or insurance companies can lawfully require the supply of information. These cases will be considered on their own merits, any request must be in writing using form VEE054 Request for Disclosure.

Under no circumstances should you supply information verbally over the phone or in person, without receiving a request in writing.

In the event of any doubt as to what information can be released, requests may be passed to, or advice taken from, compliance@veezu.co.uk .

GDPR, UK GDPR & DPA 2018

Personal data is collected, controlled, and processed in accordance with the following data protection principles:

- Lawfully, fairly and in a transparent manner;
- Only for specified, explicit and legitimate purposes;
- 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 without delay;
- 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; and
- Demonstrates compliance to all the above.

The reasons for processing personal data, how the data is used and the legal basis for processing is documented and published via:

- POL041 Passenger Privacy Notice
- POL049 Colleague and Contractor Privacy Notice

- POL063 Driver Partner Privacy Notice
- POL070 Veezu Services Colleague and Contractor Privacy Notice

DATA SUBJECT ACCESS REQUEST

To make a Data Subject Access Request ("DSAR"), individuals should send their request to Veezu Compliance at compliance@veezu.co.uk. VEE053 Subject Access Request form is available on Veezu.Net for this purpose. Proof of identification will be requested as applicable.

DSARs must legally be responded to within one month from the date that the data subject provides suitable identification. In some cases, such as where substantial amounts of the individual's data are processed, the time to respond may be extended by a further two months from the date the request is received. The requestor will be advised within one month of receiving the original request to tell them if this is the case.

If a DSAR is manifestly unfounded or excessive, we are not obliged to comply with it; it is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. The requestor will be notified if that is the case and whether we will respond to it.

DATA SECURITY

The security of personal data is taken very seriously. Internal policies and controls are in place to protect personal data against loss, accidental destruction, misuse, or disclosure and to ensure that data is not accessed inappropriately.

Further information is detailed within POL013 Information Security Policy, available on Veezu.Net.

Security procedures include:

- Door entry controls; any stranger seen in entry-controlled areas should be reported;
- Secure lockable desks and cupboards; desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential);
- Methods of disposal; paper documents should be put in the confidential waste bins. Electronic storage device should be physically destroyed when they are no longer required. Only Veezu IT & Technical can dispose of electronic devices. If you need to dispose of an electronic device a support ticket must be raised.
- Equipment; you should ensure that screens do not show confidential information to passers-by and that you log off or lock your PC when it is left unattended;
- Where we engage third parties to process personal data on our behalf, such parties do so based on written instructions, and are under a duty of confidentiality and obliged to implement appropriate technical and organisational measures to ensure the security of data. Before instructing a third party you must ensure that a Non-Disclosure Agreement or contract is in place with them.

These procedures apply both when working at a Veezu site and when working remotely in accordance with POL038 Remote Working Policy.

DATA BREACHES

Where there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will be reported to the relevant authority within 72 hours of discovery by Veezu Compliance. A record of all data breaches is maintained regardless of their effect.

If the breach is likely to result in an elevated risk to the rights and freedoms of individuals, the affected individuals will be informed and provided with information about its likely consequences as well as the mitigation measures taken.

How we process and record a data breach is set out in POL048 Data Breach Policy & Procedure and REG002 Data Breach Register.

More information on data breach procedures can be found in PRO0005 Incident Management Procedure as well as POL033 Information Security Management Policy.

DATA DISPOSAL

All records containing personal information are disposed of in line with recommended retention periods outlined by the UK ICO and Ireland's Data Protection Commission, further information can be found in POL044 Data Retention & Disposal Policy.

Beyond this, personal data will be disposed of when no longer effectively required for its purpose. The method of disposal must be appropriate to the sensitivity of the data and may include utilising confidential waste bins which are available at every site. You must be aware that when disposing of printed confidential data, the correct confidential disposal system must be used. Under no circumstances should personal data be disposed of using recycling or standard waste bins.

Note that 'deleting' a computer file does not equate to destroying the data as it can often be recovered. Please contact support@veezu.co.uk should further guidance be required.

For further information on data disposal see GUI012 Information Security Handbook and PRO008 Backup and Disaster Recovery Procedure.

TRAINING

New colleagues are briefed about their data protection responsibilities as part of the induction process.

Additional training is provided to help you understand your duties and how to comply with them on a regular basis.

NON-COMPLIANCE

If we fail to comply with our obligations under the data protection regulation, including breaching the data protection principles, data subject rights and requirements regarding international data transfers, we could be subject to significant administrative fines.

The breach of any of the instructions or procedures following from this policy will be investigated thoroughly and may result in disciplinary action in line with the POL017 Disciplinary Policy a copy of which can be found on Veezu.Net.

APPLICABLE LAW

- UK General Data Protection Regulation
- UK Data Protection Act 2018
- General Data Protection Regulation
- Irish Data Protection Act 2018

QUERIES & AMENDMENTS

Questions about this policy, or requests for further information, should be directed to Veezu Compliance at compliance@veezu.co.uk.