Hireguard

Data Protection Policy

Version 1: May 2018

1 This document 'Data Protection Policy'

This data protection policy applies to all operations by Hireguard Ltd, including their in house processes, software operations and data storage.

This policy is designed to ensure that Hireguard Ltd complies with its obligations under the Data Protection Act 2018 and how they conform to the 8 data protection principles:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
    a. at least one of the conditions in Schedule 2 is met, and
    b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This document governs all our operating procedures for our internal processes including how we manage our third party suppliers.

This is a living document and will be reviewed annually or when required. Updated copies of this document will always be recorded on our website.

2 Document Control

Version	Date	Versions
1.0	25/05/2018	Policy rewritten and replaced any previous versions issued by Hireguard Ltd. Policy includes all aspects of the business and has been rewritten to comply with new GDPR requirements.

3 In House Processes & Data Types

We hold a number of pieces of information about our clients and employees.

Data Type	Data Included	Stored using	Retention Policy
Information about bad hirers and hire companies	Hirers – names / addresses / contact information / licence information	Custom Web Application.	Indefinitely
	Hire Companies – name, address, contact information and staff membership information	Custom Web Application.	Indefinitely
Information about our employees	Job adverts / applications	Indeed Job Website	Adverts kept on file for 6 months
	Contact Details, start dates, contract, document, wage information	Basic PAYE Tools Software (all managed in house)	5 years following the employee leaving employment
	Contact details, salary and pension contribution	NEST Pensions System (3rd Party Tool)	Indefinitely
	Employee Files including payroll, contract, P45	Locked filling cabinet in HR office	5 years following the employee leaving employment
	Near misses and accidents (H&S)	File in HR office full of incident reports	Indefinitely
	Employer's Liability Insurance	Locked filling cabinet in HR office	12 months from date of issue, no previous copies kept
General Data	General contact, communications, file storage, calendar	GSuite System	7 years
	General Enquiries (Demos etc…)	GSuite System	7 years
CCTV	Data from outside building and reception area	Internal hard drive (managed by 3rd Party Company)	28 days
Finances	Purchase ledgers, payments, invoices remittance, bank reconcilliation	Quickbooks (3rd party system)	Up to 7 years inline with HMCR policies
	Annual reports & accounts	Companies House / Internal Filing Cabinet	Indefinitely

	Credit / Debit Card information	Not stored. Systems provided by 3rd party (Stripe)	As per Stripes Policy
	Fixed Asset Register	Digital in HR Team Drive	Indefinitely
	Submissions to HMRC (Tax, EU Sales List)	Quickbooks (3rd party system) File in HR Cabinet	Indefinitely
Telephone & Conferencing	Call Logs, Contact Lists	Managed using a third party service (BT Cloud Phone)	Indefinitely – Logs

3.1 Our Security Policies

The following small policies apply to all employees for the storing and protection of personal data as outlined in this policy. These security policies are mandatory.

- **Email and Communication –** We use GSuite by Google to manage all of our email, cloud and collaboration tools. All employees will use this system as part of their standard procedure. This includes email, cloud storage, hangouts and other Google related tools.
- **Passwords –** We have a policy of using and forcing complex passwords throughout all of our systems. If there is the slightest doubt that something has been compromised, then a full review of our password policy will be undertaken.
- **Employees –** We ensure that all of our employees are made aware and receive training in our data protection and IT policies.
- **Training –** We will ensure that all our employees are taught the correct procedures and will review training on an annual basis.
- **Permissions –** Staff members are only given access to resources and files as and when required. This includes customer databases.
- **Storage –** Files are to be stored using internal password protected PCs or Cloud Storage. Memory devices will not be used. Where data is printed, this will be destroyed securely using a cross cut shredder. Devices will also be encrypted incase a theft does occur
- **Data Security –** We have many policies relating to the security of our systems which are documented throughout this document
- **Physical Security –** Our office is secured and alarmed. Physical documents are further locked away in secure cabinets. There is also CCTV in use.
- **IT Security –** All of our internal systems utilise the latest software including security patches as required. A firewall blocks our incoming network. Antivirus software is installed on all machines. Please see our further security policies below in relation to our server and system security.
- **Third Party Compliance –** We ensure that all our third party suppliers are GDPR compliant.

4 Our Systems and Websites

Our Website (Hireguard.co.uk) is the frontend portal to our secure database. The database is designed to house sensitive personal information as defined under GDPR. This data includes persons and companies who have been added to the system via third party hire companies. Due to this, and to ensure the strict control of the data, we have a set of terms & conditions which apply to all users who use our Hireguard system. These terms and conditions govern access and use of the data of the system. We monitor our systems and anyone found to be breaking these terms and conditions will have their roles removed from our system.

Our website & database systems are developed and managed by a third party company, Northstone Systems Ltd. We retain all ownership and day to day running including data protection responsibilities.

We ensure that there are a number of safeguards and measures in place to protect our users when using the Hireguard system. As an overview, these are:

- Hire Companies must place a clause in their terms and conditions in order for consent to be given to share the hirers data with ourselves. We only verify hire companies who agree they have done this.
- We vet each hire company by looking at companies house and other reference agencies to ensure that they are a legitimate hire business.
- When a bad hirer is added to our system, notifications are sent to all members. These contain the region the hirer is from and their first / last name. No more information is provided in this form. Users must log into our website to view the full information.
- When searching for bad hirers, you must enter a minimum of 2 pieces of information that you know, this is the protect the identity of all members.
- If we find out that a member has misused the system, there membership can be revoked. Please refer to our terms & conditions for a full breakdown of all the membership terms

4.1 Data we hold & Backups

All data (including our code and customer databases) are stored on our secure cloud servers located in Gloucestershire. Backups that we take (backup schedule below) are stored in two locations, the first location is in the main data centre in Gloucestershire (in a different server rack), the second being a secure machine in Gateshead. Services in Gloucestershire are managed by 1&1 internet, our third party supplier.

Due to the nature of our website, all bad hirer data is fully encrypted in the database.

4.2 Third Party Services & Companies

We use a number of third party services and companies as part of our digital operations at Hireguard.

Third Party Supplier	Description
Northstone Systems Ltd	Provide and manage our Hireguard website and database.
iVech	We link data externally into the iVech Rental Management System
Mailchimp	Used for email marking from within Hireguard. Users can opt in or out of this.

5 Data Subject Access Requests

Should a member of the public request a copy of any personal information which Hireguard Ltd hold about them, they should follow the following policy. This policy can also be found on our website: https://www.Hireguard.co.uk/terms

- The individual should fill out a subject access request form at the above web address
- The request will then be acknowledged by email
- The individual's identity will then be checked to confirm they are the correct individual. This could be by them supplying an address, email address, data of birth or document based evidence
- Data will then be found and analysed to ensure we don't disclose anything unrelated to the individual
- This data will then be provided by email to the individual within 30 days of receiving the original request
- There will be no fee for this, however, if duplicate information is requested at a later date then a small administrative fee may occur.
- If your request is related to a particular company who we host the data for, you should first speak to them as they will most likely hold paper information too which we have no responsibility for.

6 Right to be forgotten

Under Data Protection, should you wish for your data to be removed from Hireguard, you'll need to follow the process below.

- We should be contacted by emailing info@hireguard.co.uk with the details of the data you are seeking to have removed.
- The director(s) will consider the request and include discussions with all relevant authorities including the ICO. We will ensure that all our statutory obligations are complied with.
- Once we've deemed what data can be deleted, we will confirm the data and timescales involved, before ensuring that the data is deleted from all the correct locations, including the destruction of paper documents if required.

7 Correcting incorrect data

If you believe some data that we hold to be incorrect, you should write to our team by emailing info@hireguard.co.uk. Once the data has been fixed, we will confirm this back.

8 Reporting a breach

At Hireguard Ltd we take data breaches very seriously and have a full policy in place should this unfortunate event occur. We have a number of policies in place to protect our systems and sensitive data, as well as our code and backend systems.

Any breach should be reported to the lead developer or company director.

Once a breach has been identified an investigation will be launched to identify what data (if any) has been damaged during the breach. We'll also consider if the data is sensitive or will result in financial loss or discrimination. If it does, the ICO will be informed within 72 hours of the breach occurring.

If the breach results in personal customer information being lost, we will work with our customers to ensure that their customers are contacted and informed about the breach and data loss.

9 Website

This document and subject access requests / right to be forgotten forms can all be found on our company website: https://www.hireguard.co.uk/terms