Northstone Systems
Data Protection Policy

Version 1.1: Updated November 2018 (original April 2018)

1 This document 'Data Protection Policy'

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

This policy is designed to ensure that Northstone Systems Ltd complies with its obligations under the Data Protection Act (soon to be the General Data Protection Regulation during 2018) and how they confirm 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, iVech System, TyreTec System, Websites, Emails and more.

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	01/04/2018	Policy rewritten and replaced any previous versions issued by Northstone Systems Ltd. Policy includes all aspects of the business and has been rewritten to comply with new GDPR requirements.
1.1	14/11/2018	Document updated to include new backup procedures across our cloud products and new third party providers.

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 our customers	billing information	Billing & Invoicing - Quickbooks (3rd party system)	Up to 7 years inline with HMCR policies
	Contact information	Hubspot	Kept forever if customer is 'live'. Disposed of after 1 year from end of customer date
	Customer Contracts	Pre November 2018 Filing Cabinet	Kept forever if customer is 'live'. Disposed of after 3 years from end of customer date
		Signable	All new contracts from November onwards are signed and stored digitally using signable
	Customer Name & Tasks / Work	Asana Project Manager App	Kept forever if customer is 'live'. Disposed of after 3 years from end of customer date
	Mailing Lists	Mailchimp once user has opted in	Indefinitely unless user requests removal
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 & GoGardless)	As per Stripes Policy As per GoCardless 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

We operate two pieces of software which have been developed by ourselves, Northstone Systems Ltd. These include the iVech Rental Software and the TyreTec Tyre Control System. This policy governs the use of these two system and our developed websites (where we host on our servers). If a website we developed is hosted by the customer, then this policy does not govern the data as security and protocols are out of our control.

4.1 Data we hold & Backups

The data we hold in our systems belong to our customers and their customers. We control the data format, but ultimately, our customers are the data controllers and should manage their data (in our system) effectively. We provide tools within our systems to make managing this data easier for our customers.

All data (including our code and customer databases) are stored on our secure cloud servers located in Gloucestershire. Backups that we take 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 further data centre in London. Services in Gloucestershire are managed by 1&1 IONOS, whilst services in London are managed by Amazon Web Services. Both are third party suppliers. They have both been checked for security and GDPR compliance.

We do not hold any payment information, long card numbers or security codes in our systems. Where a payment processor is used (PayPal, Worldpay etc…), the third party supplier details with the transactional data and financial information.

4.2 Third Party Services

Our iVech system and TyreTec system use third party suppliers and services to enhance the functionality of systems. As part of our data protection duties, we ensure that these services are compliant with GDPR, especially when we transmit data from our systems to theirs. This list documents the functionality and suppliers available.

Third Party Supplier	Description	Systems	Data
Bulk SMS Limited (Voodoo SMS)	We use an API to send data to Voodoo which sends SMS messages for our systems.	iVech	Staff Login Information Customer Reminders Mileage Requests
		TyreTec	Staff Login Information
Global Solutions Ltd (Trak Global)	Provides vehicle tracking services, we pull this information into iVech.	iVech	Vehicle Locations Driver Behaviour Scores (trak global only)
in-car cleverness limited			
Quartix			
Phaxio	Provides the ability to send a document (digitally) to a fax machine.	iVech	Customer Information
Dropbox	You can upload documents in our systems which is stored in Dropbox. Dropbox is ISO 27018 compliant.	iVech	Files could be related to Driving licences, ID, customer information, signed agreements and more.
Vehicle Data Services	Used as a VRM lookup service to pull vehicle information based on reg.	iVech	Vehicle Registration Vehicle Detailed Description
Postcode Software (Cyclops Software Ltd)	Sending a postcode to them and having the full address returned	iVech TyreTec	Postcodes Full Address Details
Hireguard Ltd	Provides known bad hirers	iVech	Personal Information
Davis (Licence Check Ltd)	Provides direct API connection to the DVLA to retrieve driving licence information	iVech	Sensitive personal information including driving licence and NI number.
Signable	Used to send contracts from iVech to end users for signing digitally.	iVech	Customer Contract including personal information and signature

5 iVech Rental Management System

Our iVech Rental Management System (or iVech for short), provides vehicle hire, leasing and management companies with an effective management system to manage all aspects of their business including but not limited to vehicles, finances, customers, bookings and much more. Due to this nature, there is a lot of sensitive information in our systems which we are responsible for as the data processor. We control the manners in which our customers store their client's information in our systems. We handle this data with the strictest of care and have a number of internal policies to manage this. It's up to our individual customers to manage how they enter that information into our system and to ensure that they have consent for the information.

In additional to our standard policies (documented above), the below policies are also in use for our iVech system.

- Where data is entered into the system about an individual, the user must confirm that consent has been obtained for marketing purposes. Consent is automatically given for the data to be entered (however, our customers should detail this in their policies)
- When a customer request comes in via email or phone, support will only be given once we have identified the company and individual concerned.
- Tools are provided for customers to manage their data including reporting on individuals who haven't hired or interacted with the company in a set period of time, so they can remove and destroy the data.
- Where data is transmitted outside the iVech system (for instance to HireGuard), a secure connection and encryption is used.

6 TyreTec Tyre Control System

Our TyreTec Control System (TyreTec for short), is a system designed to operate in the fast fit tyre industry providing our customers with a way to manage stock and invoicing. This system contains limited data in relation to personal information, but does contain supplier information, finances and vehicle registrations linked to customers. Customer data is only imputed if the customer wishes to, but majority of our customers choose not to.

In additional to our standard policies (documented above), the below policies are also in use for our TyreTec system.

- Where data is entered into the system about an individual, the user must confirm that consent has been obtained for marketing purposes. Consent is automatically given for the data to be entered (however, our customers should detail this in their policies)
- When a customer request comes in via email or phone, support will only be given once we have identified the company and individual concerned.

7 Data Subject Access Requests

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

- 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.

8 Right to be forgotten

Under Data Protection, should one of customers wish for their personal data to be forgotten (erasure), they should follow the process below:

- We should be contacted by emailing info@northstonesystems.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.

9 Correctly incorrect data

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

10 Reporting a breach

At Northstone Systems 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.

11 Website

This document and subject access requests / right to be forgotten forms can all be found on our company website: www.northstonesystems.co.uk/data-protection