Revised 15th May 2018

Minstergate Limited General Data Protection Regulation (G.D.P.R.) Policy

In order to comply with General Data Protection Regulation requirements the following confirms Minstergate Limited GDPR policy. A separate policy covering Minstergate Human Resources function is issued to all employees. This policy confirms what personal data is stored on customers/stakeholders of Minstergate including former, current and potential and how the information is used.

Information Stored

Minstergate gather sensitive personal data is order to carry out its business day to day. The sensitive data we might ask for will include the following:

- Names
- Address
- Contact telephone number
- Date of Birth
- National Insurance Number
- Birth certificate
- Marriage certificate
- Income confirmation (in the form of a payslip)
- Driving Licences

Why we ask for the information

The data requested assists us to offer our services and includes but is not limited to the following:

- Finance proposals
- Part exchange valuations
- Vehicle Sales
- Vehicle promotions
- Servicing
- MOT Testing
- Vehicles repairs both mechanical and body repairs
- Manufacturer recalls
- Parts Sales
- Driving licence checks for Insurance purposes when using Courtesy Cars

How long will the Data be held for

Minstergate will only retain your personal data for as long as it is necessary to fulfil the purposes outlined in this policy or the purposes of which you have otherwise been informed. The period we retain your personal data will be for the period required in order for us to meet our legal obligations and defend ourselves in legal disputes or fulfil Manufacturer audit requirements. If we have not received your consent for processing, or you have chosen to Opt out, the data will only be retained to the extent we are permitted to do so by law.

Computer based records:

Data stored on computers are kept in compliance with the GDPR.
Computers are only used by employees of Minstergate and employees have individual username and passwords for access.

Paper based records:

All paper based records are filed securely in a locked filing room with only senior managers having access to keys.

Who Processes the Data

All information is processed by employees of Minstergate Limited.

Training will be delivered to all employees to ensure they comply with the GDPR requirements. Training will be on-going throughout their employment with Minstergate Limited.

Transferring to Third Parties

Some personal data will be transferred to third parties such as Minstergate Insurance Company, Manufacturers, Warranty Companies, Logistics/Delivery companies, DVLA.

If information is transferred to third parties it will be for legitimate reasons or legal requirement and Minstergate Limited will never sell data to third parties for direct marketing purposes.

Credit Cards

Minstergate retain credit /debit card details however only until the payment had credited our bank account. Once the payment has been received into our account, all details will be destroyed by way of shredding.

Any credit/debit card details taken over the telephone will not be written down.

Whilst Minstergate record telephone calls for training and monitoring purposes, only Directors of Minstergate Limited has access to the recordings.

In Car Entertainment

Minstergate Limited will endeavour to ensure any sensitive personal data is removed from in-car entertainment products such as addresses in Sat Navs stored by the previous owner of a vehicle brought in for part –exchange. In these circumstances, Minstergate Limited will carry out the following checks:

- **The sales person will request the data to be removed prior to the vehicle coming in to the dealership.**
- **On receipt of the vehicle, the sales person will check the Sat-Nav to ensure any existing data is removed.**
- **On preparation of the vehicle for re-sale purposes, the technicians will check all data is removed.**

Website Users

Minstergate Limited do not use cookies on our website to track information.

Social Media

Minstergate Limited use social media for promoting its services, special offers, competitions and news.

Minstergate Limited may sometimes include images of customers on their social media site however, will never do this without gaining consent first.

Recording of Telephone Calls

Minstergate Limited will record telephone calls for training and monitoring purposes. Only Directors of Minstergate Limited have access to voice recordings and will not share details with third parties unless required to do so for legitimate purposes or lawful requirement.

Close Circuit TV

Minstergate sites all have CCTV in operation for security purposes. The images will only be passed to third parties for lawful requirement or legitimate reasons.

Marketing

Minstergate will send correspondence to existing customers based on legitimate interest. Correspondence will be in the form of emails, letters and social media. For example, Aftersales correspondence such as MOT reminders, Service reminders, Parts and Vehicle promotions will only be sent to customers who have used Minstergate for similar purchases in the past. Vehicle promotions will be assessed for suitability and relevance based upon your pervious purchase from Minstergate.

Any customer wishing to opt out of receiving correspondence from Minstergate can do so by emailing optout@minstergate.co.uk or writing to the Data Protection Officer, Minstergate, Livingstone Road, Hessle, HU13 0AB.

If you opt out of receiving correspondence from Minstergate please be aware you will be removed from our Data-base and will not receive any correspondence which includes servicing requirements.

Legitimate Interest

As mentioned above we will market our existing customers based upon legitimate interest. An existing customer means anyone who has purchased a car or a service/product from us within 5 years.

As an existing customer you can opt out of receiving any marketing from us at any time by emailing optout@minstergate.co.uk or writing to the Data Protection Officer, Minstergate, Livingstone Road, Hessle, HU13 0AB.

If you opt out of receiving correspondence from Minstergate please be aware you will be removed from our Data-base and will not receive any correspondence which includes servicing requirements.

Will all your Data be destroyed?

Upon request by our customer, Minstergate Limited will remove all personal sensitive data from our computer based records. By doing so, Minstergate Limited will cease from sending any correspondence to customers who have requested their information to be removed. However, some information may be retained in paper format such as copy invoices from vehicle sales and aftersales. Minstergate Limited will retain this data for legitimate reasons and to ensure they comply with manufacturer audit purposes and legal requirement.

Right to Request Correction, Erasure and Restriction

All customers are entitled to exercise their Right under the Data Protection Act to have any information held about them corrected, erased or restricted if the information is inaccurate or incomplete.

Such requests must be put in writing addressed to Minstergate Data Protection Officer and emailed to optout@minstergate.co.uk. The request must state which information the customer requests corrected, erased or restricted. The request will be sent to the Data Protection Officer for consideration of the request before the request is actioned.

Acknowledgement will be made within 3 days. The request will be actioned within one month however, this will be extended to two months if the request for the rectification is complex.

If it is decided by a Director no action will be taken in respect of the request for rectification, the individual will be informed in writing why.

In these circumstances individuals will be informed of their right to complain to the ICO and to a judicial remedy.

Please see below the Data Subject Request Procedure Flow Chart.

Data Subject Access Request Procedure Flow Chart

Request for information is received by Minstergate.

All requests must be directed to The Data Protection Officer for processing.

The D.P.O. Will consider:

- ✓ If the request is in writing (including email)
- ✓ Is there enough information to locate the data?
- ✓ Is there enough information to verify the identity of the person making the request?

Receipt of the request will be acknowledge within 3 working days and further information requested from the original request if not sufficient to respond with the information required.

The D.P.O. Will locate and collate the requested information.

The information will be reviewed to consider exemptions/redactions.

A copy of the disclosure bundle showing redactions will be retained for individual personnel file.

A response to the request will be made within 1 month. The data subject will be informed of the retention period and of the right to have inaccurate data corrected and their right to appeal to the ICO.

General Data Protection Regulation Data Breach Policy

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Examples of Data breaches

- Personal data breaches can include:
- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal data.

How a data breach will be dealt with

Minstergate Limited fully understand a personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. This can occur if there is a personal data breach or whenever any personal data is lost, destroyed, corrupted or disclosed, If someone accesses the data or passes it on without proper authorisation, or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

If a breach of data occurs, it must be reported to the Directors in the first instance who in turn will report the data breach to the ICO if necessary, within 72 hours of the Company being made aware of the breach.

Before reporting to the ICO consideration will be given to the likelihood and severity of the resulting risk to people's rights and freedom. If the Directors feel that there will be a risk to individual's rights and freedom the ICO will be notified.

If Directors feel there won't be a risk to individual's rights and freedom, the reasons for not reporting to the ICO will be documented for audit purposes.

If it is discovered the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the individuals will be informed without undue delay.

A record of any data breaches will be kept by the Directors.

Information to be given to the ICO

If the need occurs to report a breach to the ICO or another Supervisory authority it will contain the following:

A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned; and
- The categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer (if one is employed by Minstergate) or a contact point where more information can be obtained; This will usually be a Director or Senior Manager.
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

How the ICO Will be notified

Breaches will be phoned through on the breach on **0303 123 1113** or emailed to:

casework@ico.org.uk

Monitoring

This policy will be regularly monitored to ensure compliance and amendments implemented as required.

If you have any questions or concerns regarding any aspect of this General Data Protection Regulation Policy, please speak to the Data Protection Officer, Minstergate Limited, Livingstone Road, Hessle, HU13 0AB, Tel: 01482 333330.