GDPR

A guide for dealers

LIMITED - EXTERNAL

What you need to know

What does GDPR stand for?

General Data Protection Regulation.

When does the law surrounding personal data protection change?

25th May 2018.

What is changing?

GDPR replaces the Data Protection Act 1998. This is in response to rapid technological developments which have changed the scale and method of collecting and sharing personal data. There will now be a stronger data protection framework, backed by stronger enforcement powers, aimed at managing the risks associated with large scale data sharing in the online space.

Who does GDPR apply to?

It applies to any business handling the personal data of individuals. The GDPR applies to 'controllers' and 'processors'. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller.

What types of data does GDPR apply to?

GDPR applies to 'personal data' (such as name, contact details, address) and 'special categories of personal data' (such as health information, race or ethnicity, political opinions and sexual orientation).

What are my responsibilities under GDPR?

There are six principles you should follow when collecting and using personal data:

1. Collect and use personal information lawfully and fairly.
2. Personal information should be collected and used for clear, legitimate purposes.
3. The only personal information that should be collected and used is that which is necessary for the purposes for which it was collected.
4. Personal information must be accurate and kept up-to-date.
5. Personal information should not be kept for longer than is necessary to fulfil the purposes it was collected.
6. Personal information should be protected from unauthorised use and against accidental loss, destruction or damage.

What are the individual's rights under GDPR?

The individual has nine rights around what can and can't be done with their personal data:

1. The right to be informed – this means you must provide, at the point of collecting the data, a privacy or verbal notice informing the individual of how their personal information will be used.
2. The right to access their personal information – this means that the individual has the right to know what information you hold on them, and to request a copy of it. This information must be provided free of charge.
3. The right to get inaccurately recorded information corrected.
4. The right to erasure – this means that the individual can request that their personal data is deleted from your records, also referred to as 'the right to be forgotten'.
5. The right to restrict how their personal information is used - this means that the individual has the right to object to how you use their personal information, including for direct marketing purposes.
6. The right to receive their personal information in a legible and transferable format.
7. The right to object to the use of their personal information.
8. Rights related to automated decision making including profiling – this means the individual has the right to refuse their personal information being used to make a decision based on an automatic process without human intervention.
9. The right to compensation – this means the individual has the right to compensation if you breach GDPR requirements and it results in them suffering any harm.

Who oversees the GDPR rules?

The Information Commissioner's Office or ICO. You can find out more about the ICO and their Guide to the General Data Protection Regulation at **ico.org.uk/for-organisations**.

What are the consequences of non-compliance under GDPR?

If you find that you have breached the GDPR rules, you must inform the ICO within 72 hours.

The ICO can take the following enforcement action after investigating a data breach:

- Issue a warning notice;
- Issue a disapproval notice;
- Order you to notify the affected individuals about the personal data breach; and/or
- Issue you with a fine of up to 20 million euros or up to 4% of your annual turnover.

What are examples of personal data breaches?

- 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.

Evolution Funding's GDPR commitments to our dealer partners

Evolution Funding is currently undertaking a companywide project on GDPR to ensure that we are ready for the changes in 2018. The answers below are reflective of our current position on a number of key areas identified in GDPR.

This will be updated as we move through this project. If there is anything else you require clarification on, please contact your account manager.

Consent

Q **What personal data will be passed to us from you?**

A Proposal details and dealer set up information.

Q **How will that data then be shared by us, for example with other third parties?**

A This will be shared with our panel of funders.

Q **What is our business purpose for processing the data?**

A Data is processed for the purpose of brokering a finance application.

Q **Which part of the data life cycle does the business process relate to?**

A Processing, storage, transfer, collection.

Q **How will we notify you of the third parties to which this data will be provided and ensure such notices are kept up to date?**

A A decline or acceptance notice is issued to you on each deal. We will provide you with a copy of our Sales Procedure Guide, which is updated periodically.

Q **Is the data encrypted and if so, to what standard?**

A Resting data is encrypted, all data encryption is under review.

Q **Similarly, how will we require you to communicate and implement opt-out requests to us, where individuals with draw their consent to be contacted for marketing purposes, and how often will these opt outs be reviewed in order to maintain up to date permissions?**

A Customers can contact **unsubscribe@evolutionfunding.com**. A list of those customers will be maintained by us. Marketing permissions are stored in our systems and updated with the latest consent.

Q **What records will we provide in order to record whether consent has been provided for marketing purposes and the types of marketing, e.g. telephone, email, post?**

A We will be adding marketing permissions functionality to DealerZone, with opt-in choices.

Q **What consent do we require to cover agencies?**

A We will require explicit consent to be obtained for data processors (agencies) to be GDPR compliant.

Q **Do we use a 3rd party application/provider to process data?**

A Yes, DealTrak and Rosetta.

Q **What steps will we be putting in place to protect data subject's rights to be forgotten under GDPR?**

A Current legal and regulatory requirements to maintain customer data. Customers will contact Customer Services **customerservice@evolutionfunding.com** to request the right to be forgotten. All data is held on our secured internal systems. Our Data Protection Officer will consider all requests.

Q **What technical measures are in place to protect the data?**

A Encryption; network authentication; CCTV; password; AD authentication; access control lists; physical storage.

Q **Describe any other access controls or security measures we have in place?**

A IP banning after repeated failed logins, firewall.

Q **How is data destroyed or archived?**

A Data deletion.

Q **How long are copies of our data held for?**

A A minimum of 6 years.

Privacy Notices

Q **Our privacy notices, provided to data subjects regarding our use of their data, including its use for marketing, surveying the client and analysis.**

A Currently under review. Existing notices displayed on our website and are due to be updated before May 2018.

Q **What other parties may have access to the data or may have this data shared with them?**

A Our 3rd party funders; the FCA; collection agencies and enforcement agencies; 3rd party IT providers and credit reference agencies.

Contracts

Q **Contracts will be updated to comply with GDPR, to include clear responsibilities and the purpose and use of the data?**

A This will be in place by the end of May 2018.

Q **Do you buy or sell databases to third parties?**

A No.

Q **When will these updates be made and communicated to dealers?**

A Periodic updates will be made and communicated in your Dealer Operating Agreement.

Q **Do you subcontract any services outside the EU who may have access to this data?**

A No.

Data Location

Q **Where will data be hosted and processed by us or those acting on our behalf?**

A It will be processed by 32 funders, who are all based within the UK, are authorised and regulated by the FCA, and have notifications as a data controller with the ICO. We will be contacting them for clarification on any data taken outside the EU.

Q **Organisation's security measures we have in place?**

A Internal/external audit; automated systems monitoring; antivirus software; disaster recovery plan; segmented access control; incident response plans; awareness and training.

Q **Where is the data stored?**

A On our premises and on 3rd party premises in the UK.

- We **do not** use a cloud for storage.

Q **If data is processed outside the UK, what approach will we take to ensure customers are advised on this in our terms of privacy notice, and what contractual documentation will we have in place to cover these transfers?**

A It may sometimes be necessary to transfer personal information overseas. When this is required information is only shared within the European Economic Area (EEA). Any transfers made will be in full compliance with all aspects of GDPR.

- Data/systems **can be** accessed outside of the EU.

Sub-contractors

Q **Details of our agents and subcontractors currently involved in the processing of personal data provided by you?**

A Experian, Equifax, Call Credit and our panel of funders.

Q **How will we notify customers of these third-party processors in order to comply with GDPR?**

A Through our privacy notices.

Data Protection

Q **What processes are in place for data breaches?**

A We have an internal breaches system open to all staff. We also hold a separate breaches register. Any significant data breach will be escalated to the DPO for investigation with compliance and reported to the ICO where necessary.

Q **Have all staff received GDPR awareness training?**

A We are currently producing a GDPR training course for all staff and a workshop for managers.

Q **Have you made preparations for implementing and performing Data Protection Impact Assessments?**

A These have been completed for each department and will be reviewed annually.

Q **What processes are in place for testing, assessing and evaluating the effectiveness of technical and organisation measures for ensuring the security of processing?**

A Internal and external audits; annual management data assertions.