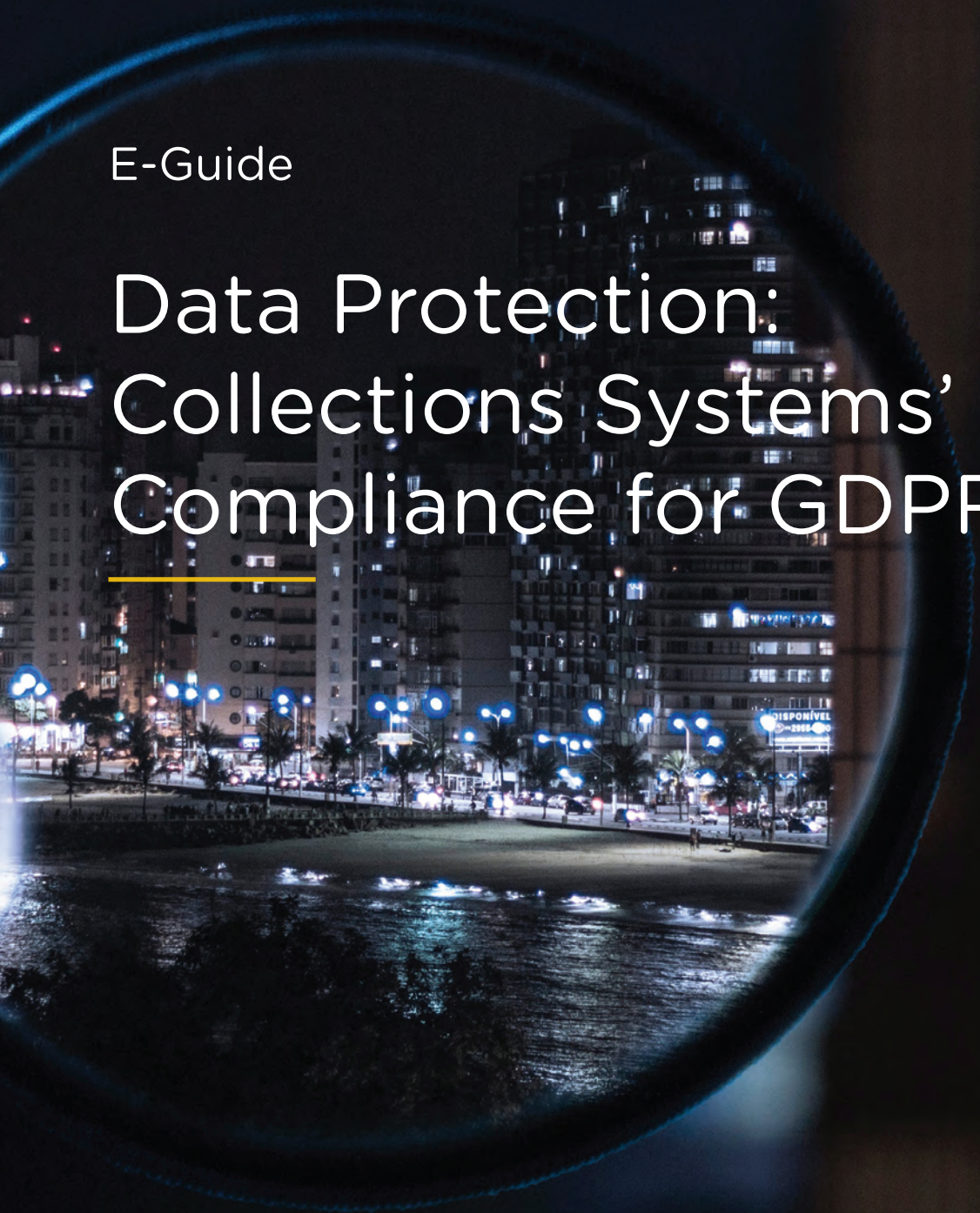
QUALCO

E-Guide

Data Protection: Collections Systems' Compliance for GDPR



REGULATION

QUALCO

CONTENTS

INTRODUCTION

The long-awaited EU General Data Protection Regulation (GDPR) comes into effect on 25 May 2018. A replacement for the 1995 EU Data Protection Directive, it is designed to significantly increase personal data protection for EU citizens.

Collections firms must ensure they have embedded the necessary controls.

The regulation increases the obligations on businesses that collect and use personal data. It builds on the 1995 Directive but includes several new provisions that elevate protection for individuals. There are also far harsher penalties for those in violation of the rules.

Organisations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements – for example not having sufficient customer consent to process data.

There is a tiered approach to fines: for example, a company can be fined 2% for not having their records in order, failing to notify the supervising authority and data subject about a breach or not conducting an impact assessment. These rules apply to both controllers and processors of data.

A key principle of GDPR is Privacy by Design. This is not a new concept but this is the first time it has been enshrined in legislation. It means data protection must be designed into systems rather than bolted on. Controllers are expected to hold and process only data absolutely necessary for their purposes, as well as limiting the access to personal data granted to processors.

The use of data is a foundation of the collections industry, with firms routinely handling and processing sensitive information. Consumers do not choose their

relationships with collection organisations, so this is likely to be an area of scrutiny by individuals, media and regulators alike.

However, this scrutiny is not a new experience for those working in collections. The stringent regulatory environment in most countries means firms are already likely to have good process in place. Customers will also not be able to demand deletion of records while accounts are active. Data portability will also have less impact than in other business sectors.

There are several areas that apply to the wider organisation beyond the collections function – and these will affect whole business policies. These include making sure you provide the right information to the right individual upon request; giving customers details about how they are using consumer data in a way that is easy to understand; transferring data to another party on a customer's request; notifying customers and authorities of breaches; and informing data subjects of the existence and consequences of any profiling activities that they carry out.

Organisations that collect and use personal data will need to put in place more robust privacy notices than have previously been required, providing more information in a more prescribed manner.

However, this document is chiefly concerned with areas specific to collections, namely: the transfer of data to third parties; customer consent; auditing; removal & deletion; access control; the right to restrict, and data portability & access. Businesses must ensure that their collections systems meet the new standards to avoid penalties and damage to their reputation.

QUALCO Collections and Recoveries manages accounts at all stages of the delinquency lifecycle. Already adapted for stringent data protection requirements, including recently-passed French data collection legislation, it has been further enriched ahead of GDPR to ensure data can be collected at the click of a button and all the relevant consents and access controls are standard.

AREAS OF FOCUS FOR COLLECTIONS FIRMS

DATA TRANSFER TO 3RD PARTIES

It's not enough for lenders and collections businesses to ensure their own compliance with GDPR, they must also ensure their third-party suppliers adhere to the legislation.

Where a data controller uses a processor for data, that processor must be able to provide "sufficient guarantees to implement appropriate technical and organisational measures" to ensure they comply with GDPR and personal details are protected.

This flows down the supply chain so that a processor cannot subcontract work to others and exchange data without the permission of the original data controller. When information is exchanged a secure network must be used.

Regulation dictates that third parties are forbidden to receive sensitive data in specific cases. It adds that password policies and authorisations must be monitored under a strict framework.

QCR Capabilities

QCR's data exchange framework uses secured protocols for the exchange of information with third parties in both directions, offering peace of mind for collections organisations.

Segments of data can be transferred to sub-contractors and information returned to the DCA and original lender with confidence. The system allows users to exclude certain accounts or portfolios so their data is not exchanged with third parties if this protection is required.

The information provided to a third party is limited to that needed for collection purposes – further protecting customer details that are not relevant to the specific job.

In addition, third parties with the ability to access system information through web applications are subject to data visibility, action authorisation restrictions and strict password policies. It will therefore be clear to the original lender who has used the data, when and for which purposes.

CUSTOMER CONSENT

Customer Consent is a significant pillar of GDPR. Organisations must obtain valid consent from individuals to justify processing their personal data. Collections professionals will already be accustomed to securing consent when contacting individuals and validating that they are speaking to the correct person.

Under GDPR, consent must be a "freely given, specific, informed and unambiguous indication of the individual's wishes". Silence, pre-ticked boxes or inactivity no longer count as consent.

The organisation must keep records to demonstrate consent has been given by the relevant individual. Consent must also be explicit when processing sensitive personal data or transferring personal data outside the EU.

QCR Capabilities

QCR comprehensively tackles this area of regulation.

Under the system customer consent for communication is not silent or automatic but user-driven. It uses communication scripts to ensure a clear, standardised approach. For activities that are configured to require customer consent, the system prompts the user to confirm consent when entering the details.

QCR provides complaint management facilities that allow customers to register any issues around inaccuracy or mistreatment of personal or transactional information.

During online communication, a special data protection authorisation (DPA) form is also used to verify that the correct person was contacted. The system will not progress to the next stage unless the customer support agent confirms consent has been obtained so there is no danger of this being forgotten.

In addition, the system monitors the best time to contact a customer and their preferred channels of communication as well as providing detailed logs of when contact was initiated and how many times the customer has been contacted.

Any changes to the system and its processes require multiple level permissions, ensuring there is transparency and accountability across all collection activities.

RECORDS OF DATA PROCESSING: AUDITING

GDPR regulation places the onus on organisations and data processors to keep their own records of data processing activities and make them available to the supervisory authority on request. This record needs to make it clear what, where, how and why data was processed.

QCR Capabilities

QCR includes the tools to configure, maintain and display a detailed audit trail of database changes down to table field level. In sensitive cases a fourth audit trail is available to identify and monitor users who search and view personal data.

The system can therefore tell not only which changes have been made but by whom.

ACCESS CONTROLS

GDPR specifies that staff and suppliers have access to no more than the data needed to do their jobs. As well as creating strict policies around this issue, organisations should invest in technology that help better manage access to data.

QCR Capabilities

The QCR system offers granular password policies, allowing companies to set password complexity, frequency of password changes and encryption. Role-based management and privileges control the actions and operations that can be taken by users - both for customer and transactional information.

In addition, Control Areas Management ensures data visibility to personnel according to their operational jurisdiction. Team members will not see any more data than they need to do their job. For example: if changes need to be made to functions and processes in the system, this doesn't require personal data to be visible and the person making those changes would not have that access.

QCR provides further checks and balances to make sure data is accurate. Even users with the clearance to modify personal data entries will not able to change information improperly. For example, if information is provided by an external source the system may require validation even if the user has the authorisation to make such changes.

The way users access the system is also monitored – showing login and logout information.

QCR web applications use encryption for information exchange with the database. PCI-compliant encryption of credit/debit card numbers is applied during online payments, card numbers are not kept in the application and online payment information with payment providers is exchanged through token-based secured protocols.

REMOVAL & DELETION: DATA ANONYMISATION

Also known as 'the right to be forgotten', one of the most significant changes under the new legislation is that customers have the right to ask companies to delete their information, even if they have previously authorised that company to use their data.

The conditions for erasure, as outlined in GDPR article 17, include the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent. Where this occurs, organisations must ensure all traces of personal information are wiped from their systems.

There are exemptions to this right – for example in relation to compliance with legal obligations. Collections teams will clearly not be forced to delete records of those from whom they are still collecting. However, once the account is closed and legislation on keeping records has been complied with, they may need to enact this process.

QCR Capabilities

Therefore, C&R firms must operate systems that are able to 'anonymise' account-level information regarding activities, notes and attachments linked to an account, after the account is closed. QCR provides this ability.

When a customer's accounts have been closed, the system can use elapsed time parameters to anonymise customer level information such as personal identification information, addresses, contacts, notes and phone numbers. If information regarding financial activities has been used these bank account-level details are also descensitised.

Under this process no physical deletion takes place in the system. Instead a global setting is used to desensitise customer information, cascading down through all the customer and account information. Only QUALCO Collections & Recoveries' customer/account internal codes remain intact. Digital files such as attachments are physically deleted and a record of these actions is maintained.

The system only allows this to take place at account level if the account is closed and at customer level if all the customer's accounts are closed. In exceptional circumstances, customers can be excluded from this process using a field in the system that will override a bulk deletion command.

Delete options are available online and can also be done in batches, subject to the user's level and permissions. Two types of deletion – ad hoc and scheduled deletions (based on elapsed times) are recorded. The user must enter the deletion reason and all actions are recorded in a table on the GDPR monitoring screen. An online deletion is treated as an urgent request, meaning organisations can fulfil their requirement to respond promptly to a customer's demand.

RIGHT TO RESTRICT

Under the GDPR legislation, the customer has the right to dispute the management of an account. This only applies in certain circumstances but while it is in force processing is restricted. The organisation may store personal data but not use it.

QCR Capabilities

The QCR system handles this by providing control areas that users cannot access. When account management needs to be suspended to deal with a customer dispute, the account is transferred to the control area.

That move ensures those managing collections or process operations do not have the ability to access the account, protecting the data while the account is restricted.

RIGHT TO ACCESS THE DATA & DATA PORTABILITY

Data 'portability' is a key element of the GDPR legislation. Customers have the right to access and transfer their data. If their requests are justified, lenders and collections teams need to be able to export personal data speedily and effectively to meet their obligations.

QCR Capabilities

When it comes to data portability or providing the information held on an individual who exercises their right to data access, QCR can export customer data in a simple click, including identity information and digital attachments such as credit agreements. This ensures it is straightforward to meet these requests and does not cost the business extra time and resources.

All actions are recorded for GDPR monitoring purposes. The same process applies for both data access and data portability requests.

GDPR also brings in new standards on profiling. However, this relates to automatic decisioning. While QCR does draw together information on customer profiles and risk – such as the number of accounts held, financial history and propensity to pay – the system does not take an automatic final decision on the best route for the customer. That final decision is taken manually by the agent.

Even so, scoring information is part of the export information that will be provided by QCR if a customer requests the data held on their file.

CONCLUSION

Not all GDPR requirements are new and most businesses should meet high standards under data protection practices in their own country or under existing EU regulation.

However, the new rules do come with severe penalties and a specific framework so businesses must ensure their systems and processes are fully compliant. The industry is asking questions about GDPR and there is an element of nervousness about the unknown, particularly for lenders who may be operating many legacy systems, with data fragmented across their businesses.

Meanwhile, the GDPR challenges for collections firms are multiple and so require a system that can manage all elements of the legislation.

Organisations must ensure the compliant transfer and **processing of data by any third parties**, with systems capable of handling and monitoring that data exchange.

Customer consent must be properly secured and recorded, it can no longer be assumed. For all data use a **clear audit trail** is essential so that the organisation can demonstrate that it meets the GDPR standards.

Removal and deletion, data portability and customer **right to access data** will all apply to the collections industry in certain cases. When these processes are necessary it is vital that organisations are able to take swift and appropriate action, again with a clear audit trail. Equally, the **right to restrict** the use of data requires a system that can ring-fence accounts and suspend the use of that data.

QUALCO Collections & Recoveries is configured for all these eventualities and offers a smooth transition process for those concerned with the requirements of GDPR.

As a high-quality end-to-end debt management system, QCR is tailored specifically to the needs of collections professionals. As well as supplying all the operation functionality needed, the system has been further adapted for GDPR – meaning collections teams can focus on their core business, safe in the knowledge they can meet their obligations.

The collections industry has long been subject to rules on the treatment of customers and their data. With the correct infrastructure, the needs of customers can be met and their data requirements and concerns handled in a straightforward, compliant manner.

QUALCO
Collections & Recoveries

QUALCO Solution ensures:

- The transfer of data to third parties is secure and actions traceable
- Customer consent is properly obtained and logged
- A clear audit trail of the way data is used
- The ability to easily provide customers with their information
- Clear access control for the parties using data
- Ad-hoc personal data desensitization when required or as part of a scheduled process

BOOK A DEMO

SHARE THIS E-GUIDE

QUALCO

QUALCO is an expert provider with more than 15 years' proven experience in enabling clients to take control of customer data across the entire credit lifecycle. Whether you are looking to modernise your internal collections platform, delve deep into the analytics of your entire debt portfolio to drive future strategy, or harness the power of external service providers, QUALCO has a solution to help you drive efficiencies and streamline your collections and recoveries operations.

UNITED KINGDOM | GREECE | CYPRUS | FRANCE | BRAZIL

QUALCO.EU