



GDPR Policy

Copyright © Smarterpay Ltd

All rights reserved. No part of this document may be disclosed to third parties or reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of Smarterpay.

Contents

Purpose.....	3
Scope	3
Responsibility and Authority	3
Our Commitment to the General Data Protection Regulation (GDPR).....	3
How has Smarterpay prepared for GDPR.....	3
Smarterpay and Bureau (Data Processor)	4
Security.....	4
Availability	4
Reliability	4
Retention and use of customer data	4
Rights of Data Subjects.....	4
Automated testing.....	5

Document Management

Version	Name	Revision Date	Change
0.1	Chris Bell	17/02/2018	Document created
1.0	Chris Bell	02/08/2019	Updated retention
1.2	Chris Bell	07/09/2019	Formatting
1.3	Edward Round	09/11/2020	Formatting

Purpose

The purpose of this document is to determine the GDPR policy within Smarterpay.

Scope

This process applies to all data and personnel in Smarterpay.

Responsibility and Authority

The Smarterpay Executive holds overall authority for this policy.

Responsibility	Appointment
Periodic review and maintenance	Managing Director
Release approval	Head of Support

Our Commitment to the General Data Protection Regulation (GDPR)

The new EU General Data Protection Regulation (GDPR) comes into force on May 25 2018. This replaces the UK Data Protection Act (DPA) and any other local equivalents in EU member states. Whilst having a similar overall aim (protecting personal data), GDPR includes new responsibilities, more stringent enforcement and substantially increased penalties.

Smarterpay is committed to high standards of information security, privacy and transparency. We comply with applicable GDPR requirements whilst processing data on behalf of our customers (as a Data Processor) and in our own handling and storage of personal information (as a Data Controller).

How has Smarterpay prepared for GDPR

There have been 2 main areas of focus in preparing for GDPR:

- Smarterpay Cloud and Bureau Services
- Internal Processes and Certifications (Data Controller)

Smarterpay has Management Systems. These management systems contain the processes developed through data classification and risk analysis to ensure that data is handled in an appropriate fashion.

We will not collect or store any unnecessary personal data relating to customers or others as part of our normal business operation. We only store sufficient information to allow us to contact and invoice customers. Any email communication sent from Smarterpay to existing customers will include an "opt out" option.

Customer information is not shared with 3rd parties.

Smarterpay and Bureau (Data Processor)

Our services may process data provided by customers on their behalf, this generally involves the receipt, storage and forwarding of files, but may also involve data transformation or reformatting (as per customer requirements).

Whilst there is a wide range of data content and formats being processed, all customer files are assumed to be of a sensitive nature and are treated as such.

Security

All data is subject to the following security practices:

- Data is secured in transit using secure communication protocols
- All customer data files are encrypted at rest on disk
- Data resides on hardware within the UK

Our services run on a separate physical network to our "Corporate" systems and are only accessible to our Managed Services support team. All of whom are trained in information security best practice.

Availability

All services are implemented using at least 2 layers of redundancy for high availability at a primary data centre. All data is backed up securely

Reliability

All services are monitored 24/7 with automated health checks, service dashboards.

File processing is monitored by our skilled Support team who will ensure that any issues are detected and followed up as a matter of urgency without compromising the security or integrity of customer data

Retention and use of customer data

Unless contractually specified, by default customer data is retained for 35 days. This allows us to assist in resolving disputes between sender and recipient regarding content.

Customer data is not used outside of the production Managed Services environment or used for any purpose other than those set out in the Managed Services contract.

The lawful basis for processing personal data is the performance and fulfilment of our contract with our customer and in certain instances the legitimate interests of Smarterpay and/or its customers.

Rights of Data Subjects

Data subjects have the right to access information held about them and the right to request that information be deleted or corrected (as appropriate). They also have the right to request that their information is transferred to another organisation. They can exercise these rights at any time by contacting us using the contact details set out below. Questions, comments, concerns and requests regarding this Privacy Statement or our collection or use of your information are welcomed and should be addressed to the email address set out below.

The Information Commissioner's Office is the UK's supervisory authority for privacy and data protection matters - for more information, please visit: www.ico.org.uk/concerns/

Automated testing

To ensure that there is no disruption to service during software upgrades, all new service releases reprocess a selection of previously processed files with the resulting output compared automatically to previous processing performed by the current service release.

This testing is automated and takes place within the same secure Managed Service environment as production processing and all customer data remains encrypted on disk.



SmarterPay Ltd
Utility House, Prospect Street, Hull, HU2 8PX
Company Registration Number: 07333064
VAT Number: GB 995 9119 56
www.smarterpay.com