sage

The General Data Protection Regulation
(GDPR) FAQ

Introduction

The General Data Protection Regulation ("GDPR") is the new legal framework that will come into effect on the **May 25, 2018** in the European Union ("EU"), and will be directly applicable in all EU Member States from that date.

The GDPR's focus is the protection of personal data, i.e. data about individuals, and builds on existing data protection laws, setting out the responsibilities of businesses in relation to the personal data they collect, hold, transmit and otherwise use. The GDPR is extra-territorial in nature and applies not just to organizations within the EU who process the data of individuals but also organizations outside the EU who offer goods or services to individuals in the EU, or who monitor the behaviour of individuals in the EU. Because the EU is a trading partner of most countries, the GDPR's wider scope means it has implications for many businesses worldwide, and will effectively require them to be compliant if they wish to operate in EU member states either directly or as a third-party for others.

This FAQ sets out some commonly asked questions asked by Sage Business Cloud People's clients and our response.

What types of data do you store?

That's up to you. Obviously, the information you require on your potential, current and former employees. You have access to fully customizable set of information fields that can be customized to ensure you collect only the minimum data necessary for your purposes, but still ensure the data is complete, adequate and accurate for your needs. Providing user self-service portals reduces your administrative overhead by allowing individuals to enter and update their own data.

How can this solution assist my GDPR compliance?

We appreciate that you are the data controller and we are a data processor, and therefore we have undergone a program to make sure that our contracts reflect our obligations to you and reflect all the GDPR requirements that apply to processors. Beyond that we have performed Product Privacy Impact Assessments to identify opportunities where we can introduce functionality that makes your job as the data controller easier, and have designed a product that enables appropriate privacy by design and default.

How do you identify privacy issues?

The Sage Business Cloud People system's internal Personal Data Protection Policy requires all new products and processes affecting personal data to undertake a Privacy Impact Assessment ("PIA") prior to launch in order to anticipate and minimize privacy risks and prevent intrusive behaviour. Where appropriate, these PIAs will be made available to clients.

What about access by your staff?

We do not access your data, unless we have your permission, for support reasons only. Sage Business Cloud People is introducing a comprehensive GDPR training program, aimed at all employees and other workers, to ensure they understand the basics of data protection law, to instil in them the nature and importance of personal data, to educate them to recognise and respond to subject access requests and learn how to report privacy breaches.

Where is my data stored?

We utilize the Salesforce platform to host your data. Our partner operates a highly resilient cloud infrastructure that we have built the Sage People platform upon. The infrastructure can be configured to be hosted locally within Europe or globally.

Does my data move internationally?

Where global requirements are in place it is the company's obligation to notify EU citizens of transfer outside of the EU and ensure adequacy measures are in place. The Salesforce platform operates mechanisms such as Privacy Shield and BCRs to legitimize international transfers and we are proud to hold TRUSTe's Privacy Seal. Sage Legal has introduced a suite of inter-company Global Data Processing and Transfer Agreements, which incorporate the requirements of the GDPR and include the use of the EC Standard Contractual Clauses for transfers of data outside the EEA. These agreements facilitate the secure movement of personal data around the Sage group of companies whilst ensuring that all processing activities comply with the GDPR

salesforce BCRs

Saleforce BCRs

Privacy Shield

TRUSTe VERIFIED

TRUSTe Certified Privacy Shield

What about back up and disaster recovery?

The Salesforce platform is a highly resilient cloud infrastructure. Back-ups are taken and we can recover your data easily in line with your retention and disposal policies. More information is available upon request.

How does the system help me to inform my users?

The organization can provide internal communications and access to policies and procedures in order to display Privacy Policies and Fair Processing notices to individuals who have their data held.

Who do you disclose data to?

That's up to you. Data from the hub network feeds into an export interface called the Sage Business Cloud People Payflow, a cloud-based system that provides feeds into external systems, such as benefits partners and payroll providers. Access and integration to personal data is controlled entirely by choices made by the business.

How long do you keep data?

Personal data may be retained for the duration of the business relationship, and retained or removed as required by law. Granular control of retention and deletion is available, where you wish to create policies to control the retention and deletion of data for each item. Sage has further information available on how long it retains data including back-up and recovery information available on request.

What if individuals put in requests for their rights, such as subject access?

You as the controller, will receive and process all requests, however we can make this easier for you. The product features a self-service interface which ensures that users have access to their own data, and users can access and update their own information as required. In addition, the reporting capabilities can be used to retrieve more comprehensive reports in the event of a formal access request. Data can be managed at a granular level in the event of a rectification or erasure request.

How is my data kept securely?

We operate appropriate security including combinations of physical, organizational and technical controls. The model is for all information is to be hosted by the Salesforce platform in a self-contained access controlled virtually separated "org". All access requests are separated with clear role based access and transactions accompanied by "Org ID" that prevents access to other company's information. More information on the Salesforce platform Security measures and certifications at https://trust.salesforce.com/.

ISO 27001

ISO 27018

SOC 1

SOC 2

SOC 3

PCI DSS

FedRAMP

DoD IL2

DoD IL4

NST 800-171

HIPAA

Financial Services Compliance - USA

Is my data encrypted in transit or at rest?

Both. We ensure that information is appropriately protected at all times. More technical information is available upon request.

What if it all goes wrong and there is a security breach?

In the unlikely event of a breach, Sage has established a global incident reporting policy and supplementary procedures, supported by Sage's risk team, enabling consistent rating and internal escalation (as required) of incidents, including those which may involve personal data

What is the wider Sage brand doing?

Sage has a project team who are focusing on the implementation of GDPR, and which is endorsed by the Sage board. In addition, Sage has robust governance procedures in place to manage the implementation of GDPR including a Data Governance Committee comprising many key stakeholders to ensure all areas of our business will be ready for GDPR from the date of enforcement in May 2018. Learn more about Sage GDPR preparations.

For more information see sage.com/gdpr

Where can I go for more information?

More information on the GDPR can be obtained from;

The text of the GDPR:
http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

The UK's regulator the Information Commissioner:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The EU guidance form the Article 29 working party:
http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

What if I have other questions?

Obviously, in order to protect your data we can't say everything in this public document. We can release more information to specific enquiries. However, you can just ask us anything, at any point! Just contact your representative, although some information may need to be released under non-disclosure agreements to protect our security environment.

About this datasheet

The information contained herein is based upon document reviews and interviews with relevant subject matter experts involved in the development and operation of the services described. The discovery process relied upon the good faith accuracy of the information provided; TrustArc has not undertaken an independent audit and does not certify the information contained in this datasheet, and has not certified the product in any way. However, the information contained herein was believed to be accurate and complete as of the time this datasheet was first published. Please note that the information provided with this paper concerning technical or legal subject matters, is for general awareness only, may be subject to change and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.

Sage legal disclaimer

The information contained in this guide is for general guidance purposes only. It should not be taken for, nor is it intended as, legal advice. We would like to stress that there is no substitute for customers making their own detailed investigations or seeking their own legal advice if they are unsure about the implications of the GDPR on their businesses.

While we have made every effort to ensure that the information provided on this website is correct and up to date, Sage makes no promises as to completeness or accuracy and the information is delivered on an "as is" basis without any warranties, express or implied. Sage will not accept any liability for errors or omissions and will not be liable for any damage (including, without limitation, damage for loss of business or loss of profits) arising in contract, tort or otherwise from the use of or reliance on this information or from any action or decisions taken as a result of using this information.

sage

www.sagepeople.com

Published: 02/18