sfG Software Ltd

GDPR Compliance Statement

May 2018

Contents

1. Introduction

The General Data Protection Regulation or GDPR is a European Union regulation that is aimed at protecting personal data of EU citizens. It replaces the existing Data Protection Act (DPA) and comes into effect on 25th May 2018. GDPR consolidates the data privacy laws across the EU region into one single regulation. Any company, be it EU or non-EU based, which processes personal data of EU individuals comes under the scope of GDPR

Simply put, individuals will now have greater say over how, why, where and when their personal data is gathered, processed and disposed of. Any organisation that works with EU residents' personal data in any manner, irrespective of location, has obligations to protect the data.

This document outlines what steps sfG Software has taken to fulfil our obligations under the GDPR legislation where we hold or process personal data on your behalf. To find out more information about GDPR, the Information Commissioner's website is an excellent resource: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

2. Our Commitment to You

sfG Software has always taken very seriously our obligations to keep your data secure. As a result, and in order to ensure we fulfil our obligations under the GDPR legislation, we have reviewed all our internal policies and we have taken steps to obtain independent third-party verification of our own security standards.

3. Data Protection and GDPR

According to the GDPR:

- A controller determines the purposes and means of processing personal data
- A processor is responsible for processing personal data on behalf of a controller
- 'Personal data' means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

In most cases our relationship with you is that you are the Data Controller and sfG Software is a Data Processor. There will also be some cases where sfG Software is a Data Controller.

We, as Data Processor, undertake to process data by: acting only on the written instructions of the Data Controller; ensuring that people processing the data are subject to a duty of confidence; taking appropriate measures to ensure the security of processing; and refraining from subcontracting the processing of your data without your consent.

4. Contracts

It is a requirement that whenever a controller uses a processor it needs to have a written contract in place, and these contracts must include various compulsory details. In cases where a data processor uses another processor (ie a 'sub-processor') then the data processor must have an appropriate contract in place with the sub-processor.

sfG Software has appropriate written contracts with all of its sub-processors.

As of 1st May 2018, sfG Software's standard client contract (ie our contract with you) contains the necessary GDPR clauses, and we have made available a contract addendum to all our

customers to ensure we have the correct contract in place going forward. If you have not received and signed one of these contracts then please get in touch at dataprotection@sfgsoftware.com.

5. Data Security

sfG Software is certified by the Cyber Essentials **Plus** scheme, providing external verification of our organisation and IT infrastructure. Cyber Essentials is a Government-backed and industry-supported scheme to help businesses protect themselves against common cyber threats. Cyber Essentials lists five technical controls (boundary firewalls and internet gateways, secure configuration, access control, malware protection and patch management) that organisations should have in place.

In order to achieve the more advanced Cyber Essentials **Plus** certification, an organisation must be audited by an independent accreditation body who tests the five key security controls and performs vulnerability and other scans. sfG Software has been certified at the more advanced "Cyber Essentials **Plus**" level so we can demonstrate a higher level of security than the basic level provides for.

In summary, these independent certifications demonstrate that we hold your data securely.

6. Sub-Processors

We use a limited number of sub-processors and we will only engage a sub-processor with a written contract which imposes the same data protection obligations as are contained in the agreement between you and us. We will only use reputable processors who are able to provide sufficient guarantees that the requirements of the GDPR will be met and the rights of data subjects protected. We will keep you informed about the sub-processors we use and we will ask your consent before appointing any new sub-processors. sfG Software has appropriate written contracts with all of its sub-processors.

7. International Transfers

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

We will not transfer data outside of the European Economic Area without your prior written consent. We are based in the UK and we always aim to store our data within the European Union. However, some organisations which provide services to us may transfer personal data outside of the EEA, but we'll only allow them to do so if your data is adequately protected.

8. Management of Personal Data Breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority within 72 hours. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, these individuals must also be informed without undue delay.

sfG Software has a clearly documented breach management process which complies with the GDPR requirements and ensures that the relevant supervisory authority (the ICO in the UK) is informed if it's likely that there will be a risk to people's rights and freedoms; and that the affected individual(s) are informed if it's likely that there will be a high risk to people's rights and freedoms.

The Managing Director has overall responsibility for assessing and managing possible breaches.

9. Internal Policies and Procedures

sfG Software has a range of internal policies covering information security, encryption, access controls, employee confidentiality, incident response management, certificate handling, etc. These policies are reviewed annually and are available on request. Staff receive regular training on these policies and are expected to read and sign these policies on an annual basis.

10. Privacy Notices

sfG Software has a number of privacy notices, depending on our relationship with you. If we are processing your data as 'data controller' then the appropriate privacy statement can be found at: https://www.sfgsoftware.com/privacy-notice.

11. Summary

This document is intended to demonstrate that we have fulfilled all our obligations under the GDPR legislation, but if you have any questions or concerns then please contact as by emailing dataprotection@sfgsoftware.com.

David Garvie
Managing Director