General Data Protection Regulation

Customer & Partner FAQ

SalamanderSoft

1. Introduction

This document is prepared by SalamanderSoft Ltd to answer customer queries around our GDPR obligations, technical and organisational measures and the Data Protection Compliance framework at SalamanderSoft Ltd.

2. GDPR Compliance Framework

	GDPR Requirements
1.	**Q – Is SalamanderSoft a Data Controller or a Data Processor when providing service to customers?** A – SalamanderSoft is the Data Processor with regards to all the services provided to customers and only acts on the instructions of the customer (Data Controller).
2.	**Q – Who is the Data Owner with respect to customer data?** A – The Data Controller is the Data Owner as they control the data and the purpose(s) of processing.
3.	**Q - Do you have a Data Protection Officer (DPO) and an Information Security Officer (ISO)?** A – SalamanderSoft will have appointed a DPO/ISO by 25th May 2018 in compliance with the GDPR requirement who can be reached at dataprotection@salamandersoft.co.uk
4.	**Q - What is your stance on GDPR?** A - We believe that data protection is very important and are committed to conforming to GDPR and have taken steps to embed GDPR in SalamanderSoft.
5.	**Q – Where are your privacy statements displayed?** A – You can access our privacy statements at https://www.salamandersoft.co.uk/privacy
6.	**Q - What steps are you taking to establish a GDPR compliance framework within your organisation?** A - We are in the final phase of our project to embed GDPR in our organisation. • All staff have been made aware of GDPR and their role and responsibilities data processors. With records of training forming part of our audit process. • Information Asset Owners have completed Data Protection Impact Assessments on our key processes and risks have been assessed. • Where applicable, identified risks have been or are in the process of being minimised by order of priority (risk score) • Copies of our Policies and Procedures have been published internally. • Privacy Notices have been updated and are publicly available on our web site. • Clients are welcome to inspect our compliance documentation and audit processes by appointment
7.	**Q - Have you had any data breaches in the last 12 months which you had to report to the Information Commissioners Office (ICO)?** A - No.
8.	**Q - What type of processing activities will be carried out?** A - SalamanderSoft is responsible for carrying out the processing activities agreed between SalamanderSoft and the Customer. These typically involve synchronising data between 2 or more of the school's systems.

9.	**Q - How do you ensure the confidentiality and security of the personal data shared with you for carrying out processing activities?** A - All processing of data is processed on servers and environments controlled by our customers.
10.	**Q - Will your organisation use the data for any other purpose than agreed?** A - No. SalamanderSoft will only act on the agreed instructions of the Data Controller.
11.	**Q - Will your organisation carry out any sort of marketing activity for the Data Controller?** A - No. This is not part of the any of the services provided by SalamanderSoft; nor do we use the customer data for our own marketing activities.
12.	**Q - What are the categories of the data processed by your organisation?** A – See our Data Processing Agreement at http://www.salamandersoft.co.uk/gdprdocs/SalamanderSoft%20Data%20Processing%20Agreement.pdf
13	**Q - What technical and organizational security measures do you have in place to protect personal data?** A- We have taken a data audit to determine where we hold personal data and all such data is is secured against unauthorised access. Access is allowed on a role basis and users must be logged in to access data.
14	**Q - Do you have any security or information management accreditation?** A – We hold the Cyber Security Essentials Certification. https://www.cyberessentials.ncsc.gov.uk/cert-search/?query=salamandersoft
15	**Q – Where do you store personal data?** A – Any personal data we hold is stored in: • Xero for billing information. https://www.xero.com/uk/campaigns/xero-and-gdpr/ • Halo ITSM for support information. https://haloitsm.com/gdpr/ • Pipedrive for lead handling. https://support.pipedrive.com/hc/en-us/articles/360000335129-Pipedrive-and-GDPR • Microsoft 365 (European data centres) for email and general documents. https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx

	Governance and Compliance
1.	**Q - Do you have a published Data Protection policy?** A - Yes.
2.	**Q - Do you have a published Information Security policy?** A - Yes.
3.	**Q - Do you have a Data Retention & Data Disposal policy?** A - Yes.
4.	**Q - Do you have policies/processes/procedures for the following areas:** **Administrator Access** **Anti-Virus** **Bring Your Own Device (BYOD)** **Cyber Security** **Data Destruction** **Data Protection**

	Employee Exit Checklist **Incident Response Plan** **Password** A - Yes, SalamanderSoft does have and maintains policies covering all the areas mentioned above. We are currently documenting our policies and processes in line with the GDPR compliance requirements.
5.	**Q - Is there a process in place to review and update these policies and procedures?** A - Yes, our documents are reviewed at least annually.
6.	**Q - How do you ensure awareness and compliance of your staff with these policies and standards?** A - All new joiners are made aware of the relevant policies for their role as part of their induction. All staff are required to undertake on-going Data Protection and Security Awareness training with includes GDPR training.
7.	**Q - Do you have an archive and back-up policy?** A - We are currently documenting the archive and back-up procedure in line with the GDPR requirements.
8.	**Q - Do you have a well-defined Leavers process in place to ensure that all access for the terminated employees is revoked?** A - Yes. Access is revoked immediately from all systems the leaver had access to.
9.	**Q - Do you have a Safe and Strong Password Policy in place?** A - Yes, this supported by technical controls and documented in the Password Policy.

	Personnel Security
1.	**Q - How many staff does your organization have?** A - 9 staff are currently employed by SalamanderSoft.
2.	**Q - Do you perform background checks on your staff?** A - All staff, both permanent and temporary, recruited within the SalamanderSoft are vetted and DBS checked.
3.	**Q - How do you ensure that your staff understand the information security requirements and practice non-disclosure?** A - As part of our user awareness training program, we have a mandatory Cyber Security training for all staff. We will be conducting GDPR training for all staff ahead of the deadline.
4.	**Q - Do you have a mandatory User Awareness & Training program for Information Security and Data Protection?** A - As part of the induction process, staff undertake computer-based learning that covers Information/Cyber Security. In addition, a further module is being developed to cover GDPR obligations and expectations which all staff will be offered.
5.	**Q - Do users have direct access to the Data Protection Officer and the Information Security Officer?** A – Yes, all existing employees and new starters can easily reach out for advice and guidance.

SalamanderSoft

3. Access to Customer Data and/or Network

	Support Services
1.	**Q - Do you need access to our network for the delivery of the support services contracted to you? If yes, please specify the procedure.** A – Yes, SalamanderSoft will need to connect to customer sites to provide installation and support. When this is required, SalamanderSoft use a secure method of connection agreed with the customer.
2.	**Q - Where will the support services be provided from?** A – All support is provided from the UK.
3.	**Q - What is the access control process in place with respect to the data shared by the customer with the support services?** A – All data is processed on customer provided servers/services and is not passed to SalamanderSoft machines. Occasionally data is saved to files on the customer machines, this typically consists of new account details, log files and any special requests by the customer. The folders used to save data are documented and permissions should be setup by the customer. There are more details in our Data Protection Agreement.
4.	**Q - How many staff will be involved in the delivery of the support services to the Data Controller?** A - SalamanderSoft has 6 members of staff in its support services.
5.	**Q - How many staff will have access to the Data Controller's data or network?** A – All support members of staff can have access, but it is agreed in advance with the customer. Some customers provide continuous anytime access.

4. Technical Measures

	Technical Security Controls
1.	**Q - Please provide an overview of the security controls in place at sites from where you provide support services.** A – **Network Security** Firewall - SalamanderSoft uses a leading third party product to ensure that all Company devices are protected with a firewall which is managed centrally. Anti-virus and Anti-malware - SalamanderSoft uses a leading third party product to ensure that all Company devices are protected with anti-virus and anti-malware, together with email processing and Web Protection against malicious websites. Patch Management - SalamanderSoft uses a leading third party product to ensure that software updates and security fixes are applied to our company devices. **Remote Access Security** SalamanderSoft uses a secure remote access application agreed with the customer for access connection to the customer network.