SGW Payroll Ltd

Third Party Supplier Compliance Questionnaire

Name of Supplier:	SGW Payroll Ltd
Service Provided:	Payroll Service

Description of the data that is processed?	For individuals: We process several pieces of personal data including name, address, contact details, Date of Birth, National Insurance, Pension, and payment details. For Businesses: We process Address, Registered address, bank details, company pay and pension information.
Where is the data stored/recorded?	The data is stored on site in our payroll system and it is also stored with our Partners Virtual Tech and Pay Dashboard. Virtual Tech backup our on-site servers to their offsite data centres and Pay Dashboard store the data in the SGW Payroll portal for end users to access.
If the data is stored in a cloud based facility, where are the servers located?	• Virtual Tech – Tier 4 datacentre (Equinix, Slough) • Pay Dashboard is a cloud based platform and all servers are maintained and held within Microsoft Azure. There are 2 servers run that are in Ireland and the Netherlands. https://azure.microsoft.com/en-gb/overview/trusted-cloud/

How long is the data retained for?	• On site – we keep copies for 6 years and the current year as per current financial and legal standards. • Virtual Tech - 3 months • Pay Dashboard - A maximum of 6 years, but each employer can decide on the period that data is visible for before it is removed or anonymised.
How and where is the data backed up?	We run many backup solutions that are described below. • Veem – data is backed up from our production servers onto our backup server using Veem. This data is kept on site and old data is removed off once a backup hits its retention period. • vCloud – Virtual Tech backup from our site to their off-site servers over a secure VPN tunnel which is then replicated between their data centres via a VPN tunnel. • Pay Dashboard – Data is backed up in real-time. All data is backed up with the EEA.
Who has access to the data?	• SGW Payroll – SGW Payroll employees and IT Support. • Virtual Tech – Virtual Tech have access to the production server once given consent, they do not have access to our Payroll software or logins. • Payrite – Payrite may be required to support our Payroll software and at times will remotely log onto a user's computer for support. This is monitored always and only with consent of our Payroll staff. • Pay Dashboard - PayDashboard support (upon prior approval), and Microsoft Azure support (in the event that permission is granted to resolve an issue beyond our control)
Who is accountable for the data?	Claire Timmis – Managing Director and Mark Haase – CEO.

Who is the data shared with?	• SGW Payroll – SGW Payroll Staff and IT Support • Payrite – Payrite may require a copy of a dataset in the event of a software issue, SGW Payroll will contact you in advance of this to make you aware. • Virtual Tech – Backups are sent off site to Virtual Tech however the underlying payroll systems are not accessible by Virtual Tech staff and will only restore any backups on request of SGW Payroll. • Pay Dashboard - The data is shared with Microsoft Azure who provide the Cloud Servers
In the event of a data breach, what is the process?	Within 24 hours of the breach being identified, SGW Payroll will inform the customer and ICO by telephone. An internal investigation will then take place to identify how the breach happened and what controls can be put into place. The customer and ICO will then be informed in writing of the outcome.
How will you notify us if a breach occurs?	SGW Payroll will telephone our named contact.
Do you sub-contract to other data processors?	No.
Please confirm that you will not allow them to access school data without prior consent from us as Data Controller	N/A
Please confirm that you have contractual arrangements in place that ensure that they are GDPR compliant, and that deal with the issues of security and breach reporting	N/A

What processes do you have in place for testing the security of your system?	• SGW Payroll – We complete planned internal tests on a number of key internal systems, as well as external firewall tests. These tests are conducted on an annual basis. • Virtual Tech – Continuous security risk assessment including quarterly vulnerability scans, regular firmware and software upgrades on network security devices and review access control • Pay Dashboard – Regular penetration testing and compliance audits with ISO and Cyber Essentials.
When was this security system last tested and what was the outcome?	• SGW Payroll – the last test on our firewall was run in February 2017 with the next schedule test to run in February 2018. Our last annual security audit was October 2017 with the next planned audit being October 2018. • Virtual Tech – Every 3 months, last time was early November, Virtual Tech completed security updates and approved access to environment • Pay Dashboard – Passed. We carry out annual penetration tests on the platform as well as annual audits for ISO:27001 and Cyber Essentials. Our next ISO Audit is due in January 2018.
What is your company's strategy for achieving compliance with the GDPR?	Consultant's advice was sought last year and a gap analysis conducted. Two Managers are subsequently acting as Project Managers to ensure compliance well in advance of May 25th.
Please provide details of your Data Protection/Information Security/Cyber Security Policy	Our new GDPR based Data Protection Policy has been prepared although this has not yet been published due to the fact that minor amendments may still be required before the May 25th deadline. Once it is completed, it will be freely available to all customers upon request.