Azolve

SaaS Subscription Agreement
Customer Agreement

Schedule D – Data Protection Policy

David Pring
1 March 2016

AZ-CSU-0100072

Azolve
1 Lonmay Road
Glasgow
G33 4EL
United Kingdom

T: +44 (0)141 773 6280
www.azolve.com

Document History

Document Type	Customer Agreement - Subscription
Document Title	SaaS Subscription Agreement – Schedule D
Customer	Customer Name
Document Version	2.0
Azolve Reference	AZ-CSU-0100072
Document Date	1 March 2016
Author	David Pring
Contact	david.pring@azolve.com
	+44 (0)141 459 0105
Reviewer(s)	Jean Leggate
Submission Dates	28 March 2016 (Version 1.0)
	30 April 2018 (Version 2.0)

Document Contents

Page

Schedule D – Data Protection Policy 4

1. Definitions 4
2. Data Protection Policy 5

Schedule D – Data Protection Policy

This schedule sets out the obligations of Azolve and its Customers with regard to data protection.

This Policy shall set out procedures which are to be followed when dealing with personal data. The procedures set out herein must be followed by Azolve, its employees, contractors, agents, consultants, partners or other parties working on behalf of Azolve.

Azolve shall ensure that it handles all personal data correctly and lawfully.

1. Definitions

In this Schedule:

A. "Agreement" means this SaaS Subscription Agreement and any associated documents referenced in the Schedule, together which form the contractual obligations between the Customer and Azolve;
B. "Azolve" means Azolve Limited an entity incorporated under the laws of England and Wales, United Kingdom; having a principal place of business at Wright Business Centre, 1 Lonmay Road, Glasgow, G33 4EL, United Kingdom, and any subsidiary or legally associated company of Azolve that is the provider of the SaaS Solution to Customer;
C. "Customer" means the company, person, organisation or legal entity ordering, using and/or paying for the subscription service for the SaaS Solution. Customer name is specified in the opening clause of this Agreement;
D. "Data Controller" means Customer;
E. "Data Processor" means Azolve;
F. "Data Protection Legislation" means any law applicable relating to the processing, privacy and use of personal data, including: (i) the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426, and any laws or regulations implementing Directive 95/46/EC (Data Protection Directive) or Directive 2002/581EC; (ii) the General Data Protection Regulation (EU) 2016/679, and/or any corresponding or equivalent national laws or regulations;
G. "Data Subject" means User;
H. "Parties" means together Azolve and Customer;
I. "Party" means either Azolve or Customer;
J. "Personal Data" means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier;
K. "SaaS Solution" means the combination of SaaS System and SaaS Services to provide a complete solution;
L. "Sensitive Personal Data" means data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.
M. "Service" means the provision of the SaaS System provided by Azolve and associated functionality provided through Third Party Software;
N. "Special Categories of Personal Data" means Sensitive Personal Data;

O. "Third Party Software" means software that Azolve uses or links to in order to provide a complete SaaS Solution, this includes, but is not limited to, online payment providers and email sending services.

2. Data Protection Policy

2.1. **The Data Protection Principles**. This Policy aims to ensure compliance with Data Protection Legislation. Data Protection Legislation sets out eight principles with which any party handling personal data must comply. All personal data:

2.1.1. Must be processed fairly and lawfully (and shall not be processed unless certain conditions are met);

2.1.2. Must be obtained only for specified and lawful purposes and shall not be processed in any manner which is incompatible with those purposes;

2.1.3. Must be adequate, relevant and not excessive with respect to the purposes for which it is processed;

2.1.4. Must be accurate and, where appropriate, kept up-to-date;

2.1.5. Must be kept for no longer than is necessary in light of the purpose(s) for which it is processed;

2.1.6. Must be processed in accordance with the rights of Data Subjects under Data Protection Legislation;

2.1.7. Must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures; and

2.1.8. Must not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.

2.2. **Responsibility of Data Controller.** It is the responsibility of Data Controller to comply with Data Protection Legislation and has full responsibility to Data Subjects to correctly gather and handle the data required to perform interactions in respect of Data Subjects' transactions with Data Controller.

Data Controller shall ensure that:

- All personal data collected and processed for and on behalf of Data Controller by any party is collected and processed fairly and lawfully;
- Data Subjects are made fully aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used;
- Personal data is only collected to the extent that is necessary to fulfil the stated purpose(s);

- All personal data is accurate at the time of collection and kept accurate and up-to-date while it is being held and / or processed;
- No personal data is held for any longer than necessary in light of the stated purpose(s);
- All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data;
- All personal data is transferred using secure means, electronically or otherwise;
- No personal data is transferred outside of the UK or EEA (as appropriate) without first ensuring that appropriate safeguards are in place in the destination country or territory; and
- All Data Subjects can exercise their rights set out in Section 3 and more fully in Data Protection Legislation.

2.3. **Rights of Data Subjects.** Under Data Protection Legislation, Data Subjects have the following rights:

- The right to be informed that their personal data is being processed;
- The right to access any of their personal data held by Data Controller within the time frame of the Data Protection Legislation;
- The right to prevent the processing of their personal data in limited circumstances; and
- The right to rectify, block, erase or destroy incorrect personal data.

It is the responsibility of Data Controller to ensure the rights of Data Subjects are not infringed.

2.4. **Personal Data**. Personal data is defined by Data Protection Legislation as data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of the Data Controller and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

Data Protection Legislation also defines “sensitive personal data” as personal data relating to the racial or ethnic origin of the Data Subject; their political opinions; their religious (or similar) beliefs; trade union membership; their physical or mental health condition; their sexual life; the commission or alleged commission by them of any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Data Controller is responsible for ensuring only personal data which is directly relevant to its dealings with a given Data Subject is held. That data will be held and processed in accordance with the data protection principles and with this Policy. The data collected, held and processed is provided in Schedule C – Privacy Policy.

2.5. **Responsibility of Data Processor.**

2.5.1. It is the responsibility of Data Processor to Process the Customer Personal Data strictly in accordance with Data Protection Legislation and on documented instruction by Customer.

2.5.2. Data Processor will have in place appropriate technical and organisational measures to ensure appropriate security of Personal Data and safeguard against any unauthorised and unlawful Processing of, and against accidental loss or destruction of, or damage to, the Personal Data. Such measures shall include but are not limited to:

2.5.2.1. appropriate measures to ensure the ongoing confidentiality, integrity, availability and resilience of the Data Processor's systems and services;

2.5.2.2. appropriate measures to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

2.5.2.3. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Personal Data

2.5.3. To notify Customer of any breach as soon as identified

2.5.4. To notify Customer of any sub-processors or sub-contractors who process data on behalf of Customer. The core sub-processors are:

- Microsoft Azure (hosting service)
- Sendgrid (email service)
- Stripe (online payment service)
- GoCardless (online payment service)
- Google (analytics)

Customer may have custom integrations with other systems via file transfer or API, this is agreed during implementation of SaaS Solution and Customer is responsible for the data protection compliance for any data outside SaaS Solution.

2.5.5. To support Customer by providing tools to manage requests from Data Subject to Data Controller through online forms and reports

2.5.6. To support Customer in requests to restrict Processing where customer is unable to do so through SaaS Solution

2.6. **Processing Personal Data.** Any and all personal data collected by Data Controller (including that detailed in Schedule C – Privacy Policy) is collected in order to ensure that Data Processor can facilitate efficient transactions with third parties including, but not limited to, it's Data Controller, partners, associates and affiliates its employees, contractors, agents and consultants. Personal data shall also be used by Data Controller in meeting any and all relevant obligations imposed by law.

Personal data may be disclosed within Data Processor. Personal data may be passed from one department to another in accordance with the data protection principles and this Policy. Under no circumstances will personal data be passed to any department or any individual within Data Processor that does not reasonably require access to that personal data with respect to the purpose(s) for which it was collected and is being processed.

Data Processor shall ensure that:

- All personal data processed for and on behalf of Data Controller by Data Processor is processed fairly and lawfully;
- All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data;
- All personal data is transferred using secure means, electronically or otherwise;
- No personal data is transferred outside of the UK or EEA (as appropriate) without first ensuring that appropriate safeguards are in place in the destination country or territory

2.7. **Data Protection Procedures.** Data Processor shall ensure that all of its employees, contractors, agents, consultants, partners or other parties working on behalf of Data Processor comply with the following when processing and / or transmitting personal data:

- All emails containing personal data must be encrypted;
- Personal data may be transmitted over secure networks only – transmission over unsecured networks is not permitted in any circumstances;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

- Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient. Using an intermediary is not permitted;
- All hardcopies of personal data should be stored securely in a locked box, drawer, cabinet or similar;
- All electronic copies of personal data should be stored securely using passwords and suitable data encryption, where possible on a drive or server which cannot be accessed via the internet; and
- All passwords used to protect personal data should be changed regularly and should not use words or phrases which can be easily guessed or otherwise compromised.

2.8. **Organisational Measures.** Data Processor shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

- A designated officer ("the Designated Officer") within Data Processor shall be appointed with the specific responsibility of overseeing data protection and ensuring compliance with Data Protection Legislation.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of Data Processor are made fully aware of both their individual responsibilities and Data Processor's responsibilities under Data Protection Legislation and shall be furnished with a copy of this Policy.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of Data Processor handling personal data will be appropriately trained to do so.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of Data Processor handling personal data will be appropriately supervised.
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
- The Performance of those employees, contractors, agents, consultants, partners or other parties working on behalf of Data Processor handling personal data shall be regularly evaluated and reviewed.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of Data Processor handling personal data will be bound to do so in accordance with the principles of Data Protection Legislation and this Policy by contract. Failure by any employee to comply with the principles or this Policy shall constitute a disciplinary offence. Failure by any contractor, agent, consultant, partner or other party to comply with the principles or this Policy shall constitute a breach of contract. In all cases, failure to comply with the principles or this Policy may also constitute a criminal offence under Data Protection Legislation.

- All contractors, agents, consultants, partners or other parties working on behalf of Data Processor handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of Data Processor arising out of this Policy and Data Protection Legislation.

- Where any contractor, agent, consultant, partner or other party working on behalf of Data Processor handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Data Processor against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

2.9. **Access by Data Subjects.** A Data Subject may make a Subject Access Request ("SAR") at any time to see the information which Data Controller holds about them.

It is the responsibility of the Data Controller to comply with Data Protection Legislation to respond to the SAR within the given timescales.

2.10. **Notification to the Information Commissioner's Office.** Data Controller is required to notify the Information Commissioner's Office that it is processing personal data.

Data Controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence. Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place. The Designated Officer shall be responsible for notifying and updating the Information Commissioner's Office.

2.11. **Implementation of Policy.** This Policy shall be deemed effective as of 01/05/2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.