RECENT UPDATES

- Section 3.3 updated to clarify ASPL responses to requests under the UK GDPR.
- Section 5.7 fixed to properly link to the Cloud Service Agreement.
- Section 5.5.3 expanded to include release-related performance testing and quality assurance testing.

INFORMATION SECURITY POLICY (2023-01-04)

At Acorah Software Products Limited ('ASPL'), we are committed to protecting your data and this Information Security Policy tells you how we secure your data. This Information Security Policy has been drafted to comply with the legal standards that currently exist in the United Kingdom and will be modified as ASPL determines is necessary to satisfy or exceed legal requirements. We reserve the right to modify this Information Security Policy at any time by notifying our customers, via the main ASPL website (www.taxcalc.com), of a new or revised Information Security Policy.

If you would like further information on this Information Security Policy or about ASPL's data security measures, we encourage you to contact compliance@taxcalc.com.

1 Introduction to ASPL Information Security

1.1 Information Commissioner's Office (ICO) registered details:

1.1.1 Our ICO registration reference is Z896266X

1.1.2 Our registered Data Protection Officer is Ian Belcher and the registered address is TaxCalc, Rubra One, Mulberry Business Park, Fishponds Road, Wokingham, RG41 2GY. Tel: 01189364855, Email: compliance@taxcalc.com

1.2 Our online Privacy Policy covers our data protection stance and provides details of data and its uses for data subjects.

1.3 ASPL only allows audits of data processing activities and those of its agents, subsidiaries and sub-contractors as far as permitted or requested by law, due to security considerations and the protection of all our other customers' data. In addition to this, a simple inspection or audit would not be feasible as there would be significant technical depth involved.

2 Information Security and ASPL Staff

2.1 ASPL staff contracts contain both confidentiality clauses and obligation to comply with information security policies clauses. The Company provides a Staff Handbook that includes a Data Protection Policy and an Electronic Usage Policy, detailing the prescribed handling of personal information. In addition, all staff are trained to adhere to our company's Privacy Policy. We run data protection awareness seminars for all staff members and update guidance when any changes or developments occur around the legislation or updated guidance from the ICO.

2.2 Lowest level permissions are routinely used regarding access or privileges within any functionality that allows interrogation of customer data.

2.3 Account access is controlled by the ASPL IT team and relevant authorisations are required

before allowing any change in access (for example, a completed new starter process), so that the employee is only given relevant access to systems. A given leaver's account access is disabled on their last day of employment and passwords are changed as required to ensure they can no longer access systems.

3 Information Security Where ASPL is the Data Controller

3.1 ASPL regularly audits its data footprint and limits data acquisition to the minimum possible.

3.2 By default, we retain data for as long as we remain in a business relationship with a customer. As soon as the relationship ends, we retain data for a further 6 years following the end of the company's financial year in order to comply with HMRC parameters on business records. Once this period elapses, all data is deleted.

3.3 ASPL responds to UK GDPR-related requests, such as Subject Access Requests and Right to be Forgotten requests, in line with the UK GDPR's requirements. Please email compliance@taxcalc.com to initiate a Subject Access Request, Right to be Forgotten request, or other UK GDPR-related request.

3.4 We do not have separate security accreditations. However, our systems are regularly scanned for vulnerabilities to adhere to PCI (Payment Card Industry) standards and our CloudConnect product undergoes penetration testing by an external third party as described in Sections 11 and 15 of the Cloud Service Agreement.

3.5 Various notification channels are monitored on a daily basis in regards to the CVE (Common Vulnerabilities & Exploits) database. All discovered instances are risk assessed to determine the severity and urgency of mitigations or updating application versions.

3.6 Software security patches are assessed and triaged as they are released, then assigned to a patch window according to the assessed risk and business impact

3.7 Our bespoke customer relationship management system (CRMS) employs a range of security measures, including restricted access, firewall protection and direct access to the data is only available to a few system administrators. We store MAC addresses used to uniquely identify customer machines and only store hashes of customer passwords. Inadvertent and malicious access to other customers data is prevented by good coding practices, preventing SQL injection attacks and all systems are internally regression tested.

3.8 Live and back-up Customer data held electronically by Acorah is normally held on our data servers at our designated datacentres within the EU, and therefore only accessible via secure remote access. Other personal data held by ASPL in electronic format will be held at our UK Head Office; our offices have door access controls and all visitors are signed in and escorted through the building.

3.9 Access to our internal network system is firewall controlled to the office and via a VPN network that uses 2FA (two factor authentication). Functionality within the internal network system is also on a least possible permission basis.

3.10 All planned Software features, releases of the Software and amendments to the Website / CRMS are reviewed by the Compliance team to ensure adherence to the relevant Acts and regulations.

3.11 All new internal uses of, or software that will interact with, Customer data are risk assessed via Data Protection Impact Assessment (DPIA) prior to implementation, so that any required adjustments can be made to the Privacy or Information Security Policies (or other relevant policies).

3.12 In the confirmed instance of a data breach that would adversely affect the personal data of a Customer, ASPL would notify You of the breach without unnecessary delay. We would also notify the ICO in such an eventuality, if it would be pertinent to do so.

3.13 The only instances of personal data that may be shared with an organisation outside of the EEA are:

3.13.1 Your registered postcode. The postcode is only shared when a customer is registering an account on the TaxCalc Website and uses the 'postcode look-up' functionality. This is provided by AFD Software, a Isle of Man based company.

3.13.2 Your IP address is provided to Maxmind Inc, a US based company (although they do have servers located in the UK). This firm states they have signed up to the EU-US Privacy Shield. This is to verify the country of purchase under the EU VAT MOSS regulations, which is needed if we are to sell software to members of EU countries.

3.13.3 Your registered email address if you opt in to any of our marketing channels. This is because we use a company called Campaign Monitor to process some of our email marketing. They are an Australian company with servers in the US, with extensive documentation covering the specific processing of data in line with EU and UK regulations. See Section 2.7 of the Privacy Policy for more details.

3.13.4 Your IP address if you complete an online survey hosted by Survey Monkey Inc. This is because Survey Monkey Inc. process some of our surveys. They are an international company with servers throughout the world, with extensive documentation covering the specific processing of data in line with EU and UK regulations. See Section 8.1.2 of the Privacy Policy for more details.

3.13.5 See Section 4 of the Privacy Policy for details regarding website usage and cookies, including the parameters for sending a variety of browsing data to OneTrust, Google Analytics, Adroll and others.

3.13.6 See Section 5 of the Privacy Policy for details regarding incoming and outgoing calls to ASPL, including the parameters for call recordings, and the transmission to and storage of data with Overline and TelcoSwitch.

3.13.7 See the Equifax Customer Licence (ECL) for details regarding usage of the Anti-Money Laundering Identity Checking Service, including all Parties responsibilities and agreements in regards to the usage of data acquired through this service.

3.14 Marketing Preferences

3.14.1 Marketing preferences are managed under the lawful basis of consent.

3.14.2 Consent is only collected directly from the data subject, usually via the TaxCalc website (as part of the registration or purchase process) but also from TaxCalc internet promotions and TaxCalc stalls at exhibitions and other functions.

3.14.3 Consent management, including withdrawal of consent, is conducted via the website

(either front end for Customers or back end for permitted customer account management staff).

3.14.4 Marketing campaigns to Data Subjects are reviewed by the Compliance team and recipients are checked against our consent options.

4 Information Security Where ASPL is the Data Processor (Core Business)

4.1 Where ASPL is a Data Processor, the security measures described in 3.1, 3.2, 3.4 to 3.6 and 3.8 to 3.12 also apply.

4.2 Additionally, where ASPL is a Data Processor, and you are the Data Controller: Wherever possible, ASPL will aid You in fulfillng Subject Access Requests and other Data Subject data management actions in line with the GDPR's timeframes and stated responsibilities.

4.3 Any subcontracted processing on behalf of Customers will be expressed within our Information Security or Privacy Policy, or legal agreements (Terms and Conditions of Sale, EULA, CSA, ECL).

5 Information Security Where ASPL is the Data Processor (TaxCalc CloudConnect®)

5.1 CloudConnect continually goes through technical updates to ensure it complies with regulatory changes and best practice standards.

5.2 Encryption

5.2.1 As per the Cloud Service Agreement, the CloudConnect databases are hosted with Mythic Beasts Ltd in the UK.

5.2.2 Each database server has disk encryption to provide Security-At-Rest. All transfers to the database are secured using SSL/TLS to provide Security-In-Transit. All encryption is to AES-256 specification. Our emergency disaster recovery methodology uses the same methods.

5.3 Access Control

5.3.1 We have privacy and non-disclosure contracts in place with our providers to ensure security of the data held on the databases. Effectively this means that our providers can and will do no more than a) host devices and b) reboot in the event of outage.

5.3.2 Our Cloud team have been allocated permissions on a least-privilege access principal (restrict access to only the level needed to fulfil job function), and successful access to any server is via explicit firewall permissions and multi-factor authentication (MFA) tooling.

5.3.3 These technical methods are coupled with extensive data protection policies in our employment contracts to ensure that staff do not access data held within Customer databases without the Customer's explicit documented instruction.

5.3.4 Each customer database is protected with unique usernames and passwords to prevent intra-server breaches. They are 'ring-fenced' as individual databases (rather than using one big database) and replicated in a master/slave fashion in order to provide redundancy.

5.4 Data Retention: We remove database backups from our servers frequently, retained as per our

Backups Attachment to the Cloud Service Agreement.

5.5 Monitoring, Testing and Remediation:

5.5.1 Issue detection (including breach/intrusion) is integrated into our 24/7 in-house monitoring and alerts; this function is handled by the Cloud team.

5.5.2 We have an automated monitoring system with hundreds of sensors implanted throughout our Cloud infrastructure. These alert us if there are any detectable problems. The quantum of 'detectable' is of course a moving target. New threats emerge constantly, the environment of the Internet changes and as we develop the service, as with any software provider, we occasionally incur bugs too. This is why we have a whole team dedicated to maintaining and developing the CloudConnect service.

5.5.3 Ongoing activities include:

- We receive notifications from a variety of security lists and websites, and all devices are patched to the latest versions on a regular patch cycle basis; this ensures that any application/package level vulnerabilities are addressed quickly.
- Reactive actions when a security problem is detected through the monitoring system.
- We perform regular penetration testing with a third party to highlight improvements, which are documented and actioned.
- Release-related performance testing and quality assurance testing, obfuscated in line with Section 6.5 of the Privacy Policy.

5.6 Cloud Server Supplier Confidence: When determining our dataserver suppliers, we engaged in a lengthy due diligence process and we have privacy and non-disclosure contracts in place to ensure security of the data held on the databases. Our suppliers do not access the unique databases; they only provide server-level support.

5.7 Further documentation on the CloudConnect Service can be found in our Cloud Service Agreement.

6 Information Security for TaxCalc Application

6.1 Data Location

6.1.1 Data entered into the Software is held in a database installed on Your local drive or network as specified upon installation, unless You are a CloudConnect user. For further information on CloudConnect please see section 5.

6.1.2 The Software includes functionality for various data to be saved externally of the database should You choose to do so, such as reports, backup files and copies of tax return files. When performing this type of action, You are able to select the location of the created file on Your local machine or network.

6.1.3 In addition to the Data Locations in 6.1.1 and 6.1.2 as part of the process of submitting a Tax Return to HM Revenue & Customs a copy of the XML submission file is created and stored in a hidden folder on the workstation used to submit the Return.