PRIVACY POLICY

This privacy policy describes the PERSONAL DATA that Chase Software Solutions Ltd ("**CHASE**" / "**WE**" / "**OUR**"/ "**US**"") gathers on or through the provision of OUR SERVICES ("**SERVICES**") and how WE use and process such information.

This policy should help you, OUR client ("**YOU**" / "**YOUR**") to better understand how WE use YOUR personal data ("**PERSONAL DATA**"), it explains in detail the types of PERSONAL DATA that WE collect, what WE use it for and who WE may share it with. If YOU have any further questions about this policy or how CHASE handles YOUR PERSONAL DATA, which is not dealt with here, please contact US using the contact details below.

Where the legal basis of consent is to be used, this will be gathered freely, and CHASE will use clear, plain language that is easy to understand, and YOU will be able to remove YOUR consent at any point.

1. **WHO WE ARE**

1.1. CHASE is the data controller of all PERSONAL DATA and data that is collected and processed about OUR customers via OUR SERVICES for the purposes of the General Data Protection Regulations ("**GDPR**").

1.2. Where YOU use the CHASE software and process the personal dataof YOUR employees, customers, suppliers, contacts, contractors and/or prospects and/or the employees of YOUR customers, suppliers, contacts, contractors and/or prospects ("**SECONDARY DATA**") and store SECONDARY DATA on either OUR hosted server or YOUR own or third-party hosted environments, YOU are considered to be the data controller and the provisions of clauses 13 and 14 will apply to YOU.

1.3. OUR company name is Chase Software Solutions Limited. WE are incorporated by the Registrar of Companies for England & Wales with registration number 9862716 and OUR registered offices are at 40 Gracechurch Street, London, EC3V 0BT.

2. **WHAT PERSONAL DATA DO WE COLLECT**

2.1. PERSONAL DATA means any information relating to YOU which allows CHASE to identify YOU.

2.2. If YOU choose to use the CHASE SERVICES, YOU must provide US with some PERSONAL DATA so that WE can provide OUR SERVICES to YOU. The PERSONAL DATA that WE collect is limited to the level WE need to deliver OUR SERVICES and is made up of the following categories:

2.2.1. names

2.2.2. email addresses

2.2.3. phone numbers

2.2.4. company names

2.2.5. company addresses

2.2.6. internet protocol (IP) addresses

2.2.7. selected usernames and passwords used to access OUR SERVICES

2.2.8. brand and product information

2.3. Other non-mandatory PERSONAL DATA may also be gathered.

3. **WHY DO WE COLLECT/PROCESS PERSONAL DATA**

3.1. WE collect/process PERSONAL DATA so that WE can provide the best possible experience when YOU, OUR client, uses OUR SERVICES. Any data collected is used to administer and deliver OUR SERVICES in accordance with the terms of YOUR written agreement with US ("**CHASE AGREEMENT**").

3.2. In addition, WE will collect/process YOUR PERSONAL DATA:

3.2.1. to comply with OUR legal obligations with regards to record retention;

3.2.2. to respond to YOUR queries and complaints;

3.2.3. for testing and applying new product or system versions, patches, updates and upgrades, and resolving bugs and other issues that YOU have reported to US;

3.2.4. to send YOU communications required by law or which are necessary to inform YOU about OUR changes to the SERVICES WE provide YOU. For example, updates to this policy;

3.2.5. to comply with OUR contractual or legal obligations to share data with law enforcement;

3.2.6. for statistical and marketing analysis, systems testing, customer surveys, maintenance and development, or in order to deal with a dispute or claim. Note that WE may perform data profiling based on the PERSONAL DATA that WE collect from YOU for statistical and marketing analysis purposes. Any profiling activity will be carried out with YOUR prior consent only and by making best endeavours to ensure that all PERSONAL DATA it is based on is accurate. By providing any PERSONAL DATA YOU explicitly agree that WE may use it to perform profiling activities in accordance with this policy;

3.2.7. to manage OUR relationship with YOU as OUR customer and to improve OUR SERVICES and enhance YOUR experience with US;

3.2.8. to protect YOUR vital interests or those of another person;

3.2.9. to protect OUR legitimate interests.

3.3. YOU are free to opt out at any time by emailing or writing to use using the contact details below.

3.4. CHASE will only process YOUR PERSONAL DATA where it has a a legal basis to do so. The legal basis will depend on the reasons WE have collected and need to use YOUR PERSONAL DATA for. For example, WE may process YOUR PERSONAL DATA to enable US to render the SERVICES in terms of the CHASE AGREEMENT.

4. RATIONAL FOR PROCESSING

WE will process PERSONAL DATA on the basis that WE have obtained YOUR consent to do so, WE have contractual obligations to fulfil which require such processing, and because WE have a legitimate interest as the legal basis to do so.

5. RETENTION OF PERSONAL DATA

5.1. The retention and/or deletion of YOUR PERSONAL DATA will be subject to OUR compliance with any legal obligations that WE may be subject to with regards to the retention and/or deletion of PERSONAL DATA and/or records as any contractual obligations that WE are bound to.

5.2. Subject to clause 5.1:

5.2.1. WE will not retain YOUR PERSONAL DATA for longer than is necessary to fulfil the purpose it was collected/ processed for. To determine the appropriate retention period, WE consider the amount, nature and sensitivity of the PERSONAL DATA, the purposes for which WE process it and whether WE can achieve those purposes through other means. WE must also consider periods for which WE might need to retain PERSONAL DATA in order to meet OUR legal obligations or to deal with complaints, queries and to protect OUR legal rights in the event of a claim being made;

5.2.2. upon the termination of the CHASE AGREEMENT WE will, at YOUR written election, either destroy or return all PERSONAL DATA to YOU. In addition, when WE no longer need YOUR PERSONAL DATA, WE will securely delete or destroy it. WE will also consider if and how WE can minimise over time the PERSONAL DATA that WE use, and if WE can pseudonymise/anonymise YOUR PERSONAL DATA so that it can no longer be associated with YOU or identify YOU, in which case WE may use that information without further notice to YOU.

6. MARKETING

WE would like to send YOU information about products and SERVICES of CHASE which may be of interest to YOU. YOU have a right at any time to stop US from contacting YOU for marketing purposes by sending US an email with YOUR request.

7. YOUR RIGHTS

7.1. Accessing or Rectifying Your Personal Data

WE want to make ensure that YOUR PERSONAL DATA is accurate and up to date and YOU have the right to request a copy and update the PERSONAL DATA that WE hold about YOU. YOU may ask US to correct or remove information YOU think is inaccurate by emailing or writing to use using the contact details below.

7.2. **Deletion**

Subject to clause 5.1, you may ask US to delete or remove PERSONAL DATA where there is no good reason for US continuing to process it. YOU also have the right to ask US to delete or remove YOUR PERSONAL DATA where YOU have exercised YOUR right to object to processing (see below).

7.3. **Object to Processing**

YOU may object to OUR processing of YOUR PERSONAL DATA where WE are relying on a legitimate interest (or that of a third-party) and there is something about YOUR particular situation which makes YOU want to object to processing on this ground. YOU also have the right to object where WE are processing YOUR PERSONAL DATA for direct marketing purposes.

7.4. **Object to Automated Decision-Making Including Profiling**

YOU can object to being the subject of any automated decision-making or US using YOUR PERSONAL DATA or profiling of YOU.

7.5. **Restriction of Processing**

YOU may ask US to suspend the processing of PERSONAL DATA about YOU, for example if YOU want US to establish its accuracy or the reason for processing it.

7.6. **Withdraw Consent**

Where YOU have provided YOUR consent to the collection, processing and/or transfer of YOUR PERSONAL DATA for a specific purpose, YOU have the right to withdraw YOUR consent for that specific processing at any time by emailing or writing to use using the contact details below. Once WE have received notification that YOU have withdrawn YOUR consent, WE will no longer process YOUR PERSONAL DATA for the purpose or purposes YOU originally agreed to, unless WE have another legitimate basis for doing so in law. YOU acknowledge that by withdrawing YOUR consent, WE may discontinue providing the SERVICES to YOU if WE required YOUR PERSONAL DATA to deliver OUR SERVICES.

7.7. **Portability**

YOU may wish to port YOUR PERSONAL DATA to another platform. This enables YOU to take YOUR PERSONAL DATA from US in an electronically useable format and to be able to transfer YOUR PERSONAL DATA to another party in an electronically useable format.

7.8. If YOU want to exercise any of YOUR rights, please email or write to US at the below address.

7.9. YOU will not have to pay a fee to access YOUR PERSONAL DATA (or to exercise any of the other rights). However, WE may charge a reasonable fee if YOUR request for access is clearly unfounded or excessive. Alternatively, WE may refuse to comply with the request in such circumstances.

8. **TO WHOM WE DISCLOSE PERSONAL DATA**

8.1. Except as described in this policy, WE will not intentionally disclose YOUR PERSONAL DATA that WE collect or store via OUR SERVICE to any third-parties without YOUR consent. WE may disclose PERSONAL DATA to third-parties if YOU consent to US doing so, as well as in the following circumstances:

8.1.1. **Unrestricted Information**

Any information that YOU voluntarily choose to include in a public area of OUR SERVICES, such as a public profile page, will be available to any visitor or user who of OUR SERVICES who access to that content.

8.1.2. **Group Companies**

Subject to the security restrictions on overseas transfers as set out in clause 8.2, YOUR PERSONAL DATA may be shared with other companies within the Chase group, both locally and internationally ("**GROUP COMPANIES**").

8.1.3. **Service Providers**

8.1.3.1. WE work with third-party service providers ("**SERVICE PROVIDERS**") who provide, for example, email hosting, core corporate applications, web hosting, maintenance, and other services to US in order for US to render OUR SERVICES to YOU. These SERVICE PROVIDERS may have access to, or

process YOUR PERSONAL DATA as part of providing their services to US. WE limit the information provided to these SERVICE PROVIDERS to that which is reasonably necessary for them to perform their functions, and OUR contracts with them require them to maintain the confidentiality of such information.

8.1.3.2. OUR SERVICE PROVIDERS include Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin, 18, D18 P521, Ireland, Provider of hosting and storing applications and associated data.

8.2. **Overseas transfers**

8.2.1. The PERSONAL DATA YOU provide may be transferred to countries outside the European Economic Area ("**EEA**") that do not have similar protections in place regarding YOUR PERSONAL DATA and restrictions on its use as set out in this policy. However, WE will take steps to ensure adequate protections are in place to ensure the security of YOUR PERSONAL DATA. The EEA comprises the EU member states plus Norway, Iceland and Liechtenstein. By submitting YOUR PERSONAL DATA, YOU consent to these transfers for the purposes specified above.

8.2.2. WE may transfer YOUR PERSONAL DATA to the following SERVICE PROVIDERS which are located outside the EEA for the following purposes:

8.2.2.1. Chase Software (Pty) Ltd, 10 Morris Street West, Rivonia, 2191, South Africa, for the purposes of performing the SERVICES;

8.2.2.2. Afrihost SP (Pty) Ltd, 376 Rivonia Boulevard, Sandton, Gauteng, South Africa, Provider of and Web Hosting; SurveyMonkey, One Curiosity Way, San Mateo, CA 94403, USA, Provider of survery tool to gain feedback from key stakeholders on satisfcation of service;

8.2.2.3. Atlassian, Level 29, 363 George Street, Sydney, NSW, 2000, Australia Provider of tool for knowledge base, issue tracking and project management;

8.2.2.4. Everlytic, Block B2, Rutherford Estate, 1 Scott Street, Waverley, Johannesburg, South Africa, 2090, Provider of tool to distribute newsletter and marketing detail to subscribed recipients;

8.2.2.5. Godaddy.com, 14455 N Hayden Rd Ste 226., Scottsdale, AZ 85260-6993, USA, Provider of SSL (Secure Sockets Layer) certificates.

8.2.3. OUR South African service providers are bound by the data protection laws of the Republic of South Africa, in particular, the Protection of Personal data Act, 4 of 2013 ("**POPI**"). POPI provides for the safeguarding of YOUR PERSONAL DATA and stipulates that YOUR PERSONAL DATA will be processed to at least similar standards as set out by the GDPR. YOU can obtain a copy of POPI at http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf.

8.2.4. If WE transfer YOUR PERSONAL DATA to any other third countries, WE will put procedures and/or contractual obligations in place to ensure that YOUR PERSONAL DATA receives a similar level of protection as set out by GDPR.

8.3. **Non-Personally Identifiable Information**

WE may make non-personally-identifiable information available to third-parties for various purposes. This data maybe automatically-collected and would be analysed to create an aggregated view of the data and ensure the reported information was anonymous.

8.4. **Law Enforcement, Legal Process and Compliance**

WE may disclose PERSONAL DATA or other information if required to do so by law or in the good-faith belief that such action is necessary to comply with applicable laws, in response to a facially valid court order, judicial or other government subpoena or warrant, or to otherwise cooperate with law enforcement or other governmental agencies, or if such disclosure is necessary to protect YOUR rights and/or the rights of others.

8.5. **Change of Ownership**

WE may disclose or otherwise transfer YOUR PERSONAL DATA to an acquirer, successor or assignee as part of any merger, acquisition, debt financing, sale of assets, or similar transaction, as

well as in the event of an insolvency, bankruptcy, or receivership in which information is transferred to one or more third-parties as one of OUR business assets and only if the recipient of the PERSONAL DATA commits to a privacy policy that has terms substantially consistent with this privacy policy.

9. **OUR DATA SECURITY**

9.1. WE have implemented appropriate technical, physical and organisational measures to protect PERSONAL DATA against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorised disclosure or access as well as all other forms of unlawful processing (including, but not limited to, unnecessary collection) or further processing.

9.2. WE use the following security procedures, technical and organisational measures to safeguard YOUR PERSONAL DATA:

9.2.1. OUR primary use and storage of PERSONAL DATA is on OUR own software which is highly encrypted and secure. All transfers of information are encrypted between OUR servers and YOUR device. Where YOU use YOUR own servers to store PERSONAL INFORMATION, YOU will be the responsible party.

9.2.2. In cases where PERSONAL DATA is being processed in third countries (except as set out above) or by third-parties, a rigorous data protection impact assessment will be performed to ensure that YOUR PERSONAL DATA is always secured.

9.2.3. OUR application platform is hosted in ISO 27001 certified secure data centres in the Northern Europe Region (Dublin, Ireland). If WE ever move the location of OUR servers, WE will notify YOU thereof in writing.

9.2.4. Firewalls, intrusion detection and prevention, anti-virus and anti-malware and backup and disaster recovery is in place to prevent data loss or deletion.

9.2.5. 24/7 security guard, closed circuit television and a door access control system to authorized personnel secures OUR offices and data centres.

9.2.6. OUR applications are engineered by industry standards to minimise security vulnerabilities and updated on a regular basis.

9.2.7. Intrusion detection and prevention secures the network traffic to the servers and applications.

9.2.8. Anti-malware and anti-virus software is deployed to all of OUR servers and WE regularly scan and update with the latest anti-malware and virus signatures.

9.2.9. WE regularly apply critical, security patches and firmware updates to operating systems and physical hardware to minimise the risk of vulnerabilities.

9.2.10. OUR employees undergo background screening and selection processes, with a restricted list of employees having access to secure areas of the applications, databases and physical infrastructure. The access to the secure areas are logged and auditable.

9.2.11. WE will use all reasonable efforts to safeguard YOUR PERSONAL DATA. However, YOU should be aware that the use of the internet is not entirely secure and for this reason WE cannot guarantee the security or integrity of any PERSONAL DATA which is transferred from YOU or to YOU via the internet.

9.2.12. WE limit access to YOUR PERSONAL DATA to those who have a genuine business need to know it. Those processing YOUR PERSONAL DATA will do so only in an authorised manner and are subject to a duty of confidentiality.

9.2.13. WE have procedures in place to deal with any suspected data security breach. WE will notify YOU and any applicable regulator of a suspected data security breach where WE are legally required to do so.

9.2.14. WE use Microsoft products including Microsoft NAV which have data encryption and the privacy notice can be seen using the following link https://privacy.microsoft.com/en-gb/privacystatement.

10. **SUB-PROCESSORS**

10.1. By YOUR acceptance of this policy, YOU confirm that YOU have given US a general authority to engage third-party processors ("**SUBPROCESSORS**") without obtaining YOUR futher written,

specificay authorisation. This authority is given on the proviso that WE will notify YOU in writing about the identity of a potential SUBPROCESSOR (and its processors, if any) before any agreements are made with the SUBPROCESSOR and before the SUBPROCESSOR processes any of SECONDARY DATA. The SUBPROCESSOR will have access to YOUR PERSONAL DATA and/or YOUR SECONDARY DATA in order to assist in the provision OUR SERVICES.

10.2. WE will conclude a written agreement with OUR SUBPROCESSOR/S, which agreement/s will subject OUR SUBPROCESSOR/S to the same level of data protection and security as US under the terms of this policy and the CHASE AGREEMENT . WE will be responsible for OUR SUBPROCESSORS' compliance with the terms of this policy and the CHASE AGREEMENT.

10.3. If YOU wish to object to the relevant SUBPROCESSOR, YOU must give US written notice thereof within seven (7) calendar days from receiving OUR notification. If YOU do not object, YOU will be deemed to have consented to the appointment of the SUBPROCESSOR.

11. **INCIDENT MANAGEMENT AND DATA BREACH NOTIFICATION**

11.1. WE promptly evaluate and respond to incidents that create suspicion of or indicate unauthorized access to or handling of YOUR PERSONAL DATA.

11.2. If a breach of data security occurs that can lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, PERSONAL DATA transmitted, stored or otherwise controlled and/or processed by US ("**PERSONAL DATA BREACH**"), WE will notify YOU thereof without undue delay, but not after 72 (seventy two) hours of becoming aware thereof.

11.3. WE will maintain a register of all PERSONAL DATA BREACHES which will, at a minimum, include the following:

11.3.1. a description of the nature of the PERSONAL DATA BREACH, including, if possible, the categories and the approximate number of affected data subjects concerned and the categories and approximate number of PERSONAL DATA records concerned;

11.3.2. a description of the likely as well as actually occurred consequences of the PERSONAL DATA BREACH;

11.3.3. a description of the measures that WE will take to address the PERSONAL DATA BREACH, including, where appropriate, measures taken to mitigate its adverse effects.

11.4. As information regarding the breach is collected or otherwise reasonably becomes available to US and to the extent permitted by law, WE will provide YOU with additional relevant information concerning the breach reasonably known or available to US.

12. **AUDIT RIGHTS**

12.1. YOU may at YOUR sole expense audit OUR compliance with the terms of this policy by sending US a written request, including a detailed audit plan, at least six weeks in advance of the proposed audit date. WE will work cooperatively with YOU to agree on a final audit plan.

12.2. The audit will be conducted no more than once during a twelve-month period, during regular business hours, subject to OUR on-site policies and regulations, and may not unreasonably interfere with OUR business activities. If YOU would like to use a third-party to conduct the audit, the third-party auditor will be mutually agreed to by the parties and the third-party auditor must execute a written confidentiality agreement that is acceptable to US. Upon completion of the audit, YOU must provide US with a copy of the audit report, which is classified as confidential information under the terms of YOUR agreement with US.

12.3. WE will contribute to such audits by providing YOU with the documentation, information and assistance reasonably necessary to conduct the audit, including any relevant records of processing activities applicable to the SERVICES. If the requested audit scope is addressed in a SOC 1 or SOC 2, ISO, NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third-party auditor within the prior twelve months and WE provide such report to YOU confirming there are no known material changes in the controls audited, YOU agree to accept the findings presented in the third-party audit report in lieu of requesting an audit of the same controls covered by the report.

13. **PROCESSING YOUR SECONDARY DATA VIA OUR HOSTED SERVICES**

13.1. **Processing Secondary Data**

13.1.1. If YOU are using OUR hosted server to store SECONDARY DATA, then WE are YOUR data processor under GDPR. Access to YOUR SECONDARY DATA is restricted by the

users YOU allow access to as well as OUR support and engineering staff that need access in order to provide the SERVICES to YOU.

13.1.2. The categories and types of SECONDARY DATA that WE may process on YOUR behalf are:

13.1.2.1. the names, addresses and contact details of YOUR employees, customers, suppliers, contacts, contractors and/or prospects;

13.1.2.2. the accounting system debtor information of YOUR customers, suppliers, contacts, contractors and/or prospects (this includes the debtor's name, address, contact details, registration number and address VAT number); and

13.1.2.3. the names, titles, designations, contact details and birthdays of the employees/representatives of YOUR customers, suppliers, contacts, contractors and/or prospects with whom YOU have contact.

13.1.3. WE will only perform processing activities that are necessary and relevant to render OUR SERVICES to YOU. WE will update this policy from time to time if there are any changes to the categories and types of SECONDARY DATA that WE may process on YOUR behalf.

13.1.4. WE will maintain a register of processing activities.

13.2. **Instruction**

13.2.1. WE will only act and process SECONDARY DATA in accordance with YOUR written instructions ("**INSTRUCTIONS**"). YOUR INSTRUCTIONS at the time when YOU conclude YOUR CHASE AGREEMENT with US will be that WE may process SECONDARY DATA with the purpose of:

13.2.1.1. rendering OUR SERVICES to YOU in accordance with the terms of the CHASE AGREEMENT; and

13.2.1.2. for statistical and marketing analysis, systems testing, customer surveys, maintenance and development, or in order to deal with a dispute or claim;

13.2.1.3. performing data profiling based on the SECONDARY DATA for statistical and marketing analysis purposes. Any profiling activity will be carried out with YOUR prior consent only and by making best endeavours to ensure that all SECONDARY DATA it is based on is accurate. By providing any SECONDARY DATA YOU explicitly agree that WE may use it to perform profiling activities in accordance with this policy

13.2.2. It is YOUR obligation to ensure that any SECONDARY DATA that YOU transfer to US is processed by YOU in accordance with applicable legislation (including GDPR), including the legislative requirements regarding the lawfulness of processing.

13.2.3. If at any time WE consider YOUR INSTRUCTIONS to be in conflict with applicable data protection legislation, WE will notify YOU thereof without undue delay.

13.3. **Confidentiality**

13.3.1. WE will treat all the SECONDARY DATA as strictly confidential information. SECONDARY DATA may not be copied, transferred or otherwise processed in conflict with YOUR INSTRUCTIONS unless YOU have agreed thereto in writing.

13.3.2. OUR employees and the employees of OUR GROUP COMPANIES (collectively, "**GROUP EMPLOYEES**") as well as OUR SERVICE PROVIDERS who have access to and process YOUR SECONDARY DATA will be subject to an obligation of confidentiality that ensures that they treat all SECONDARY DATA with strict confidentiality

13.4. **Security and Sharing of Secondary Data**

13.4.1. The security measures set out in clause 9 of this policy will apply to SECONDARY DATA.

13.4.2. SECONDARY DATA may be shared throughout the CHASE GROUP (both locally and internationally subject to the security restrictions on overseas transfers as set out in clause 8.2). Any such transfer will be done on the basis that access to SECONDARY DATA is restricted to only GROUP EMPLOYEES to whom it is necessary and relevant to process the SECONDARY DATA in order for US to render OUR SERVICES to YOU.

13.4.3. Any GROUP EMPLOYEES whose work includes processing the SECONDARY DATA will only do so in accordance with YOUR INSTRUCTIONS.

13.4.4. Your SECONDARY DATA may be exported from OUR system by OUR engineers if necessary for testing and OUR policies are in place to ensure that this data is immediately removed after any tests are completed.

13.4.5. WE work with SERVICE PROVIDERS who provide, for example, email hosting, core corporate applications, web hosting, maintenance, and other services to US in order for US to render OUR SERVICES to YOU. These SERVICE PROVIDERS may have access to, or process YOUR SECONDARY DATA as part of providing those services to US. WE limit the information provided to these SERVICE PROVIDERS to that which is reasonably necessary for them to perform their functions, and OUR contracts with them require them to maintain the confidentiality of such information.

13.4.6. OUR SERVICE PROVIDERS include Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin, 18, D18 P521, Ireland, Provider of hosting and storing applications and associated SECONDARY DATA.

13.4.7. All transfers of YOUR SECONDARY DATA is encrypted between OUR servers and the devices YOU use to access OUR software. WE cannot be held responsible for the security of YOUR devices.

13.4.8. WE may disclose SECONDARY DATA or other information if required to do so by law or in the good-faith belief that such action is necessary to comply with applicable laws, in response to a facially valid court order, judicial or other government subpoena or warrant, or to otherwise cooperate with law enforcement or other governmental agencies, or if such disclosure is necessary to protect YOUR rights and/or the rights of others.

13.5. **Data protection impact assessments and prior consultation**

If necessary, WE will assist YOU in preparing data protection impact assessments and prior consultations in accordance with articles 35 and 36 of GDPR.

13.6. **Rights of the data subjects**

13.6.1. If YOU receive a request from a data subject for the exercise of the data subject's rights under the GDPR and/or any other applicable data protection legislation and the correct and legitimate reply to such a request necessitates OUR assistance, WE will assist YOU by providing the necessary information and documentation. WE will require reasonable time to assist YOU with such requests.

13.6.2. If WE receive a request from a data subject for the exercise of the data subject's rights under the GDPR and/or any other applicable data protection legislation and such request is related to the SECONDARY DATA, WE will immediately forward the request to YOU. WE will not respond to any such request directly to the data subject.

13.7. **Secondary Data Breaches**

13.7.1. If a breach of the data security occurs that can lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, SECONDARY DATA transmitted, stored or otherwise processed on YOUR behalf ("**SECONDARY DATA BREACH**"), WE will notify YOU thereof without undue delay, but not after 72 (seventy-two) hours of becoming aware thereof.

13.7.2. WE will maintain a register of all SECONDARY DATA BREACHES which will, at a minimum, include the following:

13.7.2.1. a description of the nature of the SECONDARY DATA BREACH, including, if possible, the categories and the approximate number of affected data subjects and the categories and the approximate number of SECONDARY DATA records concerned;

13.7.2.2. a description of the likely as well as actually occurred consequences of the SECONDARY DATA BREACH;

13.7.2.3. a description of the measures that WE will take to address the SECONDARY DATA BREACH, including, where appropriate, measures taken to mitigate its adverse effects.

13.7.3. YOU, as the controller, will be required to notify any of YOUR third-parties of any such SECONDARY DATA BREACHES as contemplated in article 34 of GDPR.

13.7.4. WE will provide YOU with a copy of the register of SECONDARY DATA BREACHES if requested to do so in writing.

13.8. **Documentation of compliance**

Within a reasonable time of receipt of YOUR written request, WE will provide YOU with documentation substantiating that WE complied with OUR obligations in respect of the processing of SECONDARY DATA as contemplated in:

13.8.1. this policy;

13.8.2. YOUR INSTRUCTIONS; and

13.8.3. the applicable data protection laws (including GDPR) in respect of the processing of SECONDARY DATA.

13.9. **Return or Deletion of Secondary Data**

13.9.1. The retention and/or deletion of YOUR SECONDARY DATA will be subject to OUR compliance with any legal obligations that WE may be subject to with regards to the retention and/or deletion of SECONDARY DATA and/or records as well as any contractual obligations that WE are bound to.

13.9.2. Subject to clause 13.9.1, upon the termination of the CHASE AGREEMENT WE will, at YOUR written election, either destroy or return all SECONDARY DATA to YOU. In addition, when WE no longer need the SECONDARY DATA to provide OUR SERVICES, WE will securely delete or destroy it.

14. **PERSONAL DATA AND SECONDARY DATA IN YOUR HOSTED ENVIRONMENT**

14.1. If YOU are using YOUR own or a third-party hosted environment, then WE will not have access to YOUR PERSONAL DATA and/or SECONDARY DATA unless you specifically grant us such access. WE will require access to YOUR hosted environment to implement upgrades, new systems, customisations and/or fixes.

14.2. WE will not process and/or remove to YOUR PERSONAL DATA and/or SECONDARY DATA from your hosted environment without YOUR permission.

14.3. If WE remove to YOUR PERSONAL DATA and/or SECONDARY DATA from your hosted environment, it will be for the purposes of implementing new systems, upgrades and/projects with regards to our SERVICES. Once the implementation is complete WE will migrate all of YOUR PERSONAL DATA and/or SECONDARY DATA back onto YOUR hosted environment and we will delete all records and copies of YOUR PERSONAL DATA and/or SECONDARY DATA that was used for the implementation from our systems.

14.4. If requested by YOU, we will create a backup of YOUR PERSONAL DATA and/or SECONDARY DATA, which backup will be stored on YOUR hosted environment.

15. **SYSTEMS OPERATIONS DATA PROCESSING TERMS**

"**SYSTEMS OPERATIONS DATA**" includes log files, event files, and other trace and diagnostic files, as well as statistical and aggregated information that relates to the use and operation of OUR SERVICES, and the systems and networks that the SERVICES run on.

15.1. **Responsibility and Purposes for Processing Personal Data and/or Secondary Data Contained in Systems Operations Data**

15.1.1. WE are responsible for processing PERSONAL DATA and/or SECONDARY DATA that may be incidentally contained in SYSTEMS OPERATIONS DATA. WE may collect or generate SYSTEMS OPERATIONS DATA for the following purposes:

15.1.1.1. to help keep OUR SERVICES secure, including for security monitoring and identity management;

15.1.1.2. to investigate and prevent potential fraud or illegal activities involving OUR systems and networks, including to prevent cyber-attacks and to detect bots;

15.1.1.3. to administer OUR back-up disaster recovery plans and policies;

15.1.1.4. to confirm compliance with licensing and other terms of use (license compliance monitoring);

15.1.1.5. research and development purposes, including to analyse, develop, improve and optimize OUR SERVICES;

15.1.1.6. to comply with applicable laws and regulations and to operate OUR business, including to comply with legally mandated reporting, disclosure or other legal process requests, for mergers and acquisitions, finance and accounting, archiving and insurance purposes, legal and business consulting and in the context of dispute resolution.

15.1.2. For PERSONAL DATA and/or SECONDARY DATA contained in SYSTEMS OPERATIONS DATA collected in the EU, OUR legal basis for processing such information is OUR legitimate interest in performing, maintaining and securing OUR products and SERVICES and operating OUR business in an efficient and appropriate manner. PERSONAL DATA and/or SECONDARY DATA may also be processed based on OUR legal obligations or legitimate interest to comply with such legal obligations.

15.2. **Sharing Personal Data and/or Secondary Data Contained in Systems Operations Data**

15.2.1. PERSONAL DATA contained in SYSTEMS OPERATIONS DATA may be shared as contemplated in clause 8.

15.2.2. SECONDARY DATA contained in SYSTEMS OPERATIONS DATA may be shared as contemplated in clause 13.4.

15.2.3. When third-parties are given access to PERSONAL DATA and/or SECONDARY DATA contained in SYSTEMS OPERATIONS DATA, WE will take the appropriate contractual, technical and organisational measures to ensure, for example, that such data is only processed to the extent that such processing is necessary, consistent with this policy and in accordance with applicable law.

15.3. **Security**

WE have implemented appropriate technical, physical and organisational measures to protect PERSONAL DATA and SECONDARY DATA contained in SYSTEMS OPERATIONS DATA against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorised disclosure or access as well as all other forms of unlawful processing (including, but not limited to, unnecessary collection) or further processing.

15.4. **Rights of Data Subjects**

15.4.1. To the extent provided under applicable laws, you may request to access, correct, update or delete PERSONAL DATA contained in SYSTEMS OPERATIONS DATA in certain cases, or otherwise exercise YOUR rights as contemplated in clause 7 by sending US a request to do so at the below address.

15.4.2. If YOU receive a request from a data subject for the exercise of the data subject's rights under the GDPR and/or any other applicable data protection legislation with regards to SECONDARY DATA contained in SYSTEMS OPERATIONS DATA and the correct and legitimate reply to such a request necessitates OUR assistance, WE will assist YOU by providing the necessary information and documentation. WE will require reasonable time to assist YOU with such requests.

15.4.3. If WE receive a request from a data subject for the exercise of the data subject's rights under the GDPR and/or any other applicable data protection legislation with regards to SECONDARY DATA contained in SYSTEMS OPERATIONS DATA, WE will immediately forward the request to YOU. WE will not respond to any such request directly to the data subject.

16. **CONTACT US**

16.1. OUR company address is 40 Gracechurch Street, London, EC3V 0BT

16.2. OUR postal address is 16 The Mall, Surbiton, KT6 4EQ

16.3. OUR telephone number is +44 7943 549271

16.4. OUR email address is jamie@Chasesoftware.biz

17. **CONTACTING THE REGULATOR**

17.1. If YOU have any complaints regarding OUR compliance with this policy, please contact US first. WE will investigate and attempt to resolve any complaints and disputes regarding OUR privacy practices.

17.2. If YOU feel that YOUR PERSONAL DATA has not been handled correctly, or YOU are unhappy with OUR response to any requests YOU have made to US regarding the use of YOUR PERSONAL DATA, YOU have the right to lodge a complaint with the Information Commissioner's Office.

17.3. YOU can contact them by calling 0303 123 1113. Or go online to www.ico.org.uk/concerns (please note WE can't be responsible for the content of external websites).

18. **CHANGES TO POLICY**

18.1. WE may change this policy from time to time and any changes will be communicated to YOU by way of an e-mail or a notice on OUR website.

18.2. YOU will be requested to accept any changes to this policy if YOU wish to continue using the SERVICES. If YOU do not accept such changes YOU will not be able to access OUR SERVICES, system and/or software. If YOU do not want to agree to changes to this policy, YOU can request an account deletion. Note that YOUR refusal to accept any changes to this policy will not absolve YOU of YOUR obligations as per the CHASE AGREEMENT.

18.3. This privacy policy was last updated on 2018/06/18.

19. **LIMITATION OF LIABILITY**

19.1. Whilst CHASE uses adequate security and technological measures to safeguard YOUR PERSONAL DATA and SECONDARY DATA, CHASE will not be liable for any breach or compromise of personal information and/or breach of privacy beyond the reasonable control of CHASE and which may include, but is not limited to:

19.1.1. acts of terrorism, cyber-terrorism, cyber-extortion, cyber-attacks, viruses, malware, malicious code, logic bombs, spyware, worms, trogan horses, hacking, vis-majors, criminal actions by third-parties unrelated to CHASE;

19.1.2. network disruptions beyond CHASE'S reasonable control and which may occur on YOUR computer systems and any failure by YOU, YOUR employees and/or YOUR service providers to ensure that YOU implement adequate security safeguards to protect YOUR PERSONAL DATA and SECONDARY DATA on YOUR computer systems and devices;

19.1.3. unauthorised user access by YOU and password protection breaches which is no fault on the part of CHASE;

19.1.4. where YOU are the responsible party and host YOUR own PERSONAL DATA and/or SECONDARY DATA on YOUR own servers or use YOUR own service providers to host YOUR PERSONAL DATA and/or SECONDARY DATA and any breach is not caused by any fault of CHASE.

19.2. If YOU are hosting YOUR own servers where PERSONAL DATA and/or SECONDARY DATA is stored, YOU are solely responsible for ensuring that YOU have adequate technological measures in line with good industry practice to ensure the protection of YOUR PERSONAL DATA and SECONDARY DATA and YOU hereby indemnify and hold harmless, CHASE, its directors, employees and/or agents from any damages, claims, expenses and/or legal costs, which may arise now or in the future, as a result of a breach of security to YOUR own systems, which does not arise as a result of CHASE'S acts or omissions.

20. **YOUR OBLIGATIONS**

20.1. YOU warrant in favour of CHASE that YOU have obtained the consent of any third-party for the use of that third party's PERSONAL DATA and/or SECONDARY DATA in this way, or otherwise that such processing is lawful. Except in the event of CHASE'S gross negligence or fraud , YOU hereby indemnify and holds harmless CHASE, its directors, employees and/or contractors, now and in the future from any claim, expense, damages and legal costs arising from:

20.1.1. YOUR failure to obtain the third-party's consent to lawfully process their PERSONAL DATA and/or SECONDARY DATA;

20.1.2. YOUR breach of any relevant data protection legislation in the EEU, including GDPR.

20.2. You consent to CHASE retaining back-ups of YOUR PERSONAL DATA and SECONDARY DATA for no less than 6 (six) years after termination of the CHASE AGREEMENT or for longer as may be required in law for the retention of records. CHASE provides no warranty in respect of the effectiveness of such backups.

20.3. To the extent that YOU collect SECONDARY DATA in terms of the CHASE AGREEMENT, YOU will be responsible for all obligations of a controller in terms of GDPR.

20.4. YOU undertake to advise CHASE as soon as reasonably possible of if the Regulator investigates YOU or makes a ruling against YOU pertaining to YOUR failure or contravention of GDPR.

20.5. When accessing, dealing with, collecting and/or processing PERSONAL DATA and/or SECONDARY DATA, using the SERVICES, YOU must at all times:

20.5.1. not request, collate, process and/or store PERSONAL DATA and/or SECONDARY DATA which is not necessary for the lawful purpose for which the PERSONAL DATA and/or SECONDARY DATA is required;

20.5.2. obtain written permission from the database subject for the collection, collation, processing and/or disclosure of any PERSONAL DATA and/or SECONDARY DATA;

20.5.3. not use the PERSONAL DATA and/or SECONDARY DATA for any purpose other than for the disclosed purpose for which the database subject gave their written permission;

20.5.4. keep a record of the PERSONAL DATA and/or SECONDARY DATA and the reason for which the PERSONAL DATA and/or SECONDARY DATA was collected, for as long as the PERSONAL DATA and/or SECONDARY DATA is used by YOU;

20.5.5. keep a record of all security breaches with regards to PERSONAL DATA and SECONDARY DATA;

20.5.6. not disclose the PERSONAL DATA and/or SECONDARY DATA to any third-party, unless permitted by legislation to do so or authorised in writing by the database subject to do so. A record of any such disclosure must be kept for as long as the PERSONAL DATA and/or SECONDARY DATA is used by the database subject and the record must contain details on the reasons for the disclosure, the date of disclosure and the entity or person to whom disclosure was made;

20.5.7. delete and/or destroy any PERSONAL DATA and/or SECONDARY DATA that becomes obsolete. Prior written approval must be obtained from the database subject before any such deletion and/or destruction takes place; and

20.5.8. treat all PERSONAL DATA and/or SECONDARY DATA in a consistent and confidential manner.