GDPR Data Agreement for Partners

GDPR - Data Protection Agreement for Partners

Between:

CeeJay Software Limited
23 Melville Street
Edinburgh
Scotland
EH3 7PE

Registered in Scotland under registration number SC390957

and

Partner Name:

Company Address:

Registered In:

Company Registration Number:

Your Email Address:

1. Introduction

1.1 We are committed to safeguarding the privacy of all individuals and partners whose personal data we store and process; in this notice we explain how we will handle your and your customers personal data.

1.2 This notice applies where we are acting as a data controller with respect to your personal data; in other words, where we determine the purposes and means of the processing of that personal data.

1.3 In this notice, "we", "us" and "our" refer to CeeJay Software Limited

2. How we use your personal data

2.1 In this section 2 we have set out:

(a) the general categories of personal data that we may process;(b) in the case of personal data that we did not obtain directly from you, the source and specific categories of that data;(c) the purposes for which we may process personal data; and(d) the legal bases of the processing.

2.2 We may process your partner account data ("account data"). The account data may include your name, postal address, telephone number and email address. The source of the account data is you or your employer. The account data may be processed for the purposes of providing our services, ensuring the security of our services, maintaining back-ups of our databases and communicating with you. The legal basis for this processing is consent OR our legitimate interests, namely the proper administration of our business OR the performance of a contract between you and us and/or taking steps, at your request, to enter into such a contract.

2.3 We may process your personal data that are provided in the course of the use of our services ("service data"). The service data may include cloud server usage, storage usage and login activity. The source of the service data is you or your employer. The service data may be processed for the purposes of providing our services, ensuring the security of our services, maintaining back-ups of our databases and communicating with you. The legal basis for this processing is consent OR our legitimate interests, namely the proper administration of our business OR the performance of a contract between you and us and/or taking steps, at your request, to enter into such a contract.

2.4 We may process information relating to transactions, including purchases of goods and services, that you enter into with us ("transaction data"). The transaction data may include your contact details, your card details and the transaction details. The transaction data may be processed for the purpose of supplying the purchased goods and services and keeping proper records of those transactions. The legal basis for this processing is the performance of a contract between you and us and/or taking steps, at your request, to enter into such a contract and our legitimate interests, namely our interest in the proper administration of our business.

2.5 We may process information that you provide to us for the purpose of subscribing to our email notifications and/or newsletters ("notification data"). The notification data may be processed for the purposes of sending you the relevant notifications and/or newsletters. The legal basis for this processing is consent OR the performance of a contract between you and us and/or taking steps, at your request, to enter into such a contract.

2.6 We may process information contained in or relating to any communication that you send to us ("correspondence data"). The correspondence data may include the communication content and metadata associated with the communication. The correspondence data may be processed for the purposes of communicating with you and record-keeping. The legal basis for this processing is our legitimate interests, namely the proper administration of our business and communications with users.

2.7 We may process any of your personal data identified in this notice where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. The legal basis for this processing is our legitimate interests, namely the protection and assertion of our legal rights, your legal rights and the legal rights of others.

2.8 We may process any of your personal data identified in this notice where necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, or obtaining professional advice. The legal basis for this processing is our legitimate interests, namely the proper protection of our business against risks.

2.9 In addition to the specific purposes for which we may process your personal data set out in this section 2, we may also process any of your personal data where such processing is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

2.10 Please do not supply any other person's personal data to us, unless we prompt you to do so.

3. Providing your personal data to others

3.1 We may disclose your personal data to any member of our group of companies (this means our subsidiaries) insofar as reasonably necessary for the purposes, and on the legal bases, set out in this notice.

3.2 We may disclose your personal data to our insurers and/or professional advisers insofar as reasonably necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, obtaining professional advice, or the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

3.3 Financial transactions relating to services may be handled by our payment services providers depending on how you pay these are GoCardless and/or Stripe. We will share transaction data with our payment services providers only to the extent necessary for the purposes of processing your payments, refunding such payments and dealing with complaints and queries relating to such payments and refunds. You can find information about the payment services providers' privacy policies and practices at gocardless.com and stripe.com.

3.5 In addition to the specific disclosures of personal data set out in this section 3, we may disclose your personal data where such disclosure is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person. We may also disclose your personal data where such disclosure is necessary for the establishment, exercise or defence of legal claims,

whether in court proceedings or in an administrative or out-of-court procedure.

4. International transfers of your personal data

4.1 In section 4, we provide information about the circumstances in which your personal data may be transferred to countries outside the European Economic Area (EEA).

4.2 We have offices and facilities in Scotland (Head Office), Data Centres in London, Frankfurt, Amsterdam, Prague, USA and New Zealand. The European Commission has made an "adequacy decision" with respect to the data protection laws of each of these countries. Transfers to each of these countries will be protected by appropriate safeguards, namely the use of standard data protection clauses adopted or approved by the European Commission.

4.3 Data locations of our services
All data being transmitted is encrypted, all data stored is encrypted by several layers for all our services only a few members of CeeJay Software in our head office in Scotland can access the settings and view log files which shows the status of any backups. Only the end user (customer) can decrypt their encrypted file-level data.

Our Website:

www.ceejay.com and backupintelligence.com and protectedintelligence.com

Is located in the UK and or Europe with all data encrypted at transmission and at rest, only the team in Scotland has access to the website data. The website contains the order form for all our services which are Backup Intelligence, Sync Intelligence, Three Steps Web and CrashPlan in CeeJay Cloud. We request your name, company name, postal address, telephone number, email address, invoice email address, and plan you wish to purchase, as well as the IP address and date created, which are all stored. We also use Google Analytics on the website for analytics of it's performance, visitors, browsers, page views.

Backup Intelligence - Cloud Backup / Protected Intelligence:

Backup Intelligence is CeeJay Software’s own cloud backup solution to back up servers, endpoints, cloud to cloud, virtual machines, Protected Intelligence for Office 365 and Google Suite.

The master server for all accounts is located in Europe which stores your username and encrypted login information along with all the settings used in Backup Intelligence or Protected Intelligence.

The storage servers which the end-users select to store their encrypted backup data are located in one of three locations of the end-users choosing which are either UK (London), Europe (Amsterdam) or USA (Ashburn).

5. Retaining and deleting personal data

5.1 This section 5 sets out our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of personal data.

5.2 Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

5.3 We will retain your personal data as follows:

(a) Invoicing Details are sent to our partners are retained for a minimum period of 7 years following creation date to allow for financial inspections in the UK.

5.4 In some cases it is not possible for us to specify in advance the periods for which your personal data will be retained. In such cases, we will determine the period of retention based on the following criteria:

(a) the period of retention of backup data will be determined based on the specific storage period set upon by the user / administrator or partner in the backup solutions.(b) If you delete or close your backup account or remove a device from the backup plan all data is automatically purged after 48 hours and is non-recoverable.(c) If you unselect a file, files, folders or drive or path from your backup selection then the backup for that item will be purged from the backup archive at our cloud using the retention settings you have chosen in either Backup Intelligence, Sync Intelligence or in CrashPlan.

5.5 Notwithstanding the other provisions of this section 5, we may retain your personal data where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

6. Security of personal data

6.1 We will take appropriate technical and organisational precautions to secure your personal data and to prevent the loss, misuse or alteration of your personal data.

6.2 All data we hold is stored and transmitted by us using several layers of encryption.

6.3 All our passwords used to access our software and IT systems are not

susceptible to being guessed, administrator passwords are between 40 and 8000 characters long and with Backup Intelligence, Sync Intelligence, Intercom we also use 2 factor authentication on all administration accounts.

6.4 Customers and our partners are responsible for keeping the passwords confidential and we will not ask you for your passwords (except when you log in to our solutions). Backup Intelligence will have a new web based console later in May 2018 for end users and partners with that we will require ultra strong passwords and will use 2 factor authentication.

6.5 In Backup Intelligence it is impossible for you or us to request a password reset unless you have chosen that option to allow a password reset through the account settings in the desktop client.

6.6 All CrashPlan password resets go back to the user's email address.

6.6 All our systems for administration access by us use Apple macOS or iOS devices running on our secure internal network. We do not use public wifi networks. For example, if our CEO were away from the office checking email, a dedicated 4G or secure satellite network is used. All our devices are encrypted and do not show notifications when locked and are tracked globally by our email platform run out of our data centre in Frankfurt. All our devices can be remotely wiped if necessary.

6.7 We use a few other solutions to help us and through these systems some information is stored:

KashFlow is our accounts system which stores the invoicing details of our partners, which is located in London U.K. (Rackspace Data Centre) and stores customer order details. This information is retained for 7 years for our financial checks.

Details Stored in KashFlow: Your Name, Company Name, Postal Address, Telephone Number, Solution Ordered, Pricing, Invoice Date, Payment Method, Payment Date, Account Notes. There is no bank account information stored i.e. account number, credit or debit card in KashFlow.

GoCardless is our Direct Debit payment processor. This is stored in the UK and only used when partners set up to pay in the UK by Direct Debit.

Details Stored in GoCardless are: Your Name, Address, Email Address and Financial Details (such as account holder name, account number, sort code) of the GoCardless end-customer (i.e. the purchaser of services/ goods from a merchant using GoCardless to collect payments).

Stripe is our credit or debit card payment processor, which is only used when partners pay by debit or credit card. EU-U.S. and Swiss-U.S. Privacy Shield Framework: https://stripe.com/privacy-shield-policy

Intercom which is used when partners place a support ticket. Intercom uses Amazon AWS and is located in USA: https://www.intercom.com/security

ISLOnline is used when we run a screenshare to support a customer or partner with an issue to allow us remotely control their computer.

Zoom is used when we do webinars. Their data centre is located in USA with all data encrypted end-to-end and destroyed at the end of the webinars. For recordings we will download them and make them available through our website. EU-U.S. and Swiss-U.S. Privacy Shield Framework

CCTV Our premises are protected inside and outside with Netatmo CCTV Cameras which record video and audio and process face recognition, car recognition and animal recognition, all data is encrypted and stored in our London data centre.

Bank Details if partners pay directly into our bank account then the payment details are held by the Royal Bank of Scotland (RBS)

7. Amendments

7.1 We we publish changes to this notice on our website at www.ceejay.com

8. Your rights

8.1 In this section 8, we have summarised the rights that you have under data protection law. Some of the rights are complex, and not all of the details have been included in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.

8.2 Your principal rights under data protection law are:

(a) the right to access;(b) the right to rectification;(c) the right to erasure;(d) the right to restrict processing;(e) the right to object to processing;(f) the right to data portability;(g) the right to complain to a supervisory authority; and(h) the right to withdraw consent.

8.3 You have the right to confirmation as to whether or not we process your personal data and, where we do, access to the personal data, together with certain additional information. That additional information includes details of the purposes of the processing, the categories of personal data concerned and the recipients of the personal data. Providing the rights and freedoms of others are not affected, we will supply to you a copy of your personal data. The first copy will be provided free of charge, but additional copies may be subject to a reasonable fee.

You can request access to your personal data by visiting us at https://

help.ceejay.com and putting in a request to view your data.

8.4 You have the right to have any inaccurate personal data about you rectified and, taking into account the purposes of the processing, to have any incomplete personal data about you completed.

8.5 In some circumstances you have the right to the erasure of your personal data without undue delay. Those circumstances include: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; you withdraw consent to consent-based processing; you object to the processing under certain rules of applicable data protection law; the processing is for direct marketing purposes; and the personal data have been unlawfully processed. However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for the establishment, exercise or defence of legal claims.

8.6 In some circumstances you have the right to restrict the processing of your personal data. Those circumstances are: you contest the accuracy of the personal data; processing is unlawful but you oppose erasure; we no longer need the personal data for the purposes of our processing, but you require personal data for the establishment, exercise or defence of legal claims; and you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your personal data. However, we will only otherwise process it: with your consent; for the establishment, exercise or defence of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important public interest.

8.7 You have the right to object to our processing of your personal data on grounds relating to your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task carried out in the public interest or in the exercise of any official authority vested in us; or the purposes of the legitimate interests pursued by us or by a third party. If you make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.

8.8 You have the right to object to our processing of your personal data for direct marketing purposes (including profiling for direct marketing purposes). If you make such an objection, we will cease to process your personal data for this purpose.

8.9 You have the right to object to our processing of your personal data for scientific or historical research purposes or statistical purposes on grounds

relating to your particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

8.10 To the extent that the legal basis for our processing of your personal data is:
(a) consent; or(b) that the processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract, and such processing is carried out by automated means, you have the right to receive your personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.

8.11 If you consider that our processing of your personal information infringes data protection laws, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. You may do so in the EU member state of your habitual residence, your place of work or the place of the alleged infringement.

8.12 To the extent that the legal basis for our processing of your personal information is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

8.13 You may exercise any of your rights in relation to your personal data by written notice to us OR by email correspondence OR by telephone correspondence, in addition to the other methods specified in this section 8.

9. Our details

9.1 Our full legal name is CeeJay Software Limited

9.2 We are registered in Scotland under registration number SC390957, and our registered office is at

CeeJay Software Limited
23 Melville Street
Edinburgh
Scotland
EH3 7PE

VAT Registration Number GB 116 1130

9.3 Our principal place of business is at CeeJay Software Limited, at the above address.

9.4 You can contact us:

(a) by post, to the postal address given above;(b) using our website at

https://ceejay.com;(c)

10. Representative within the European Union

10.1 Our representative within the European Union with respect to our obligations under data protection law is our CEO and you can contact our representative through the above contact information.

11. Data protection officer

11.1 Our data protection officer's is our CEO, Mr Craig Laird Jamieson.

CeeJay Software Limited
23 Melville Street
Edinburgh
Scotland
EH3 7PE

Your legal name

Signed by Craig Jamieson
Signed On: 21st January 2020