Privacy and Security Statement

Introduction

CubeBackup Inc. is strongly committed to protecting the privacy and confidentiality of our customers, business partners, and other individuals. We have implemented technical, administrative, and physical measures to safeguard all information that we may collect. This statement explains what data CubeBackup processes, how CubeBackup processes it, and for what purposes.

Definitions

- "**CubeBackup**", "**we**", "**us**" and "**our**" refer to CubeBackup Inc.
- "**Products**", "**software**" refer to the software distributed by CubeBackup.
- "**You**" and "**your**" refer to a customer, supplier, business partner, a website visitor, or a representative of any other organization with whom CubeBackup has a business relationship.
- "**Customers**" refers to organizations who use our products to backup their Google Workspace or Microsoft 365 data.
- "**Backup data**" refers to customers' Google Workspace or Microsoft 365 data backed up by products.
- "**Google Workspace or Microsoft 365 data**" refers to customer's business data stored on Google Workspace domain(s) or Microsoft 365 organization(s).
- "**Site**" and "**website**" refer to the website https://www.cubebackup.com.

Business Personal Information

What does CubeBackup mean by your Business Personal Information?

In the course of CubeBackup's interactions with you as a customer, supplier, Business Partner, a website visitor, or a representative of any other organization with whom CubeBackup has or contemplates a business relationship, CubeBackup may collect and process personal information about you. CubeBackup refers to this information as "Business Personal Information". The Business Personal Information does not mean backup data or any data stored on Google Workspace domain(s) or Microsoft 365 organization(s). The Business Personal Information that CubeBackup processes may include:

- Business contact information, such as your name and your business e-mail address, physical address and telephone number;
- Information with respect to your use of the CubeBackup products and website; and
- Purchasing information, including Google Workspace or Microsoft 365 domain name(s), number of users, credit card details, purchase date, and other financial-related information collected in support of business transactions.

How do we use Business Personal Information?

CubeBackup uses the data we collect to provide you with rich, interactive experiences. In particular, we use data to:

- Provide our products to customers, which includes updating, securing, and troubleshooting our software. It also includes sharing data, when this is necessary to provide service or carry out the transactions you request.
- Provide support to customers. We use data to troubleshoot and diagnose product problems, provide other customer care and support services, including to help us provide, improve, and secure the quality of our products.
- Improve and develop our products. We use data to continually improve our products, including adding new features or capabilities.
- Protecting rights and property. We use data to detect and prevent fraud, resolve disputes, and protect our property.

When we process personal data about you, we do so with your consent and/or as required to provide the products you use, operate our business, meet our contractual and legal obligations, protect the security of our systems and our customers, or fulfill other legitimate interests of CubeBackup.

Our general principles for processing Business Personal Information.

Here are CubeBackup's general principles which apply to its processing of Business Personal Information. The term "processing" includes collecting, using, disclosing, storing, accessing or transferring your Business Personal Information. CubeBackup states that we will:

- Collect and process Business Personal Information fairly, lawfully and in a transparent manner.
- Process Business Personal Information which is adequate, relevant to and not excessive for the purpose for which it is processed.
- Keep Business Personal Information as accurate, complete and up to date as necessary for the purpose for which it is processed.
- Implement appropriate technical and organizational measures to safeguard Business Personal Information.

When will your Business Personal Information be shared outside CubeBackup?

Your Business Personal Information may only be communicated by CubeBackup to a third party (for example a CubeBackup Business Partner or third party contracting on CubeBackup's behalf) under certain conditions:

- You have provided free and informed consent regarding the communication;
- To process credit card or other financial transactions;
- It is required or authorized by applicable law; or
- It is necessary for investigatory or statutory audit purposes or to obtain legal advice.

Google Workspace or Microsoft 365 data

Our products are the CubeBackup software used to backup Google Workspace or Microsoft 365 data for our customers. As a backup solution provider, CubeBackup commits to ensuring the security, privacy, and integrity of customer's Google Workspace or Microsoft 365 data and backup data.

How is backup data stored?

Our products are installed on the customer's machine and back up the customer's Google Workspace or Microsoft 365 data from Google's and Microsoft's servers to the customer's own storage. CubeBackup states that:

1. Backup data processed by our products is stored solely on storage our customers control, either using on-premises storage belonging to the customer, or the customer's private cloud storage. No Google Workspace or Microsoft 365 data or backup data for any Google and Microsoft account, including Google Drive files, Shared drives files, Gmail messages, Google Contacts, Google Calendar data, Google Sites files, Microsoft SharePoint data, OneDrive files, Outlook Mail messages, Outlook Calendar data or Outlook People contacts, will be collected or stored by CubeBackup.
2. No Google Workspace or Microsoft 365 backup data will be accessed or transferred to CubeBackup or any third party.
3. No configuration settings, metadata, private key files, or log files for our products will be collected, stored, or transferred by CubeBackup, unless specifically provided by our Customers for technical support purposes.

4. No login credentials or any account information of our products will be collected, stored, or transferred by CubeBackup.
5. No Google Workspace and Microsoft 365 account information (for example, Google Workspace and Microsoft 365 email addresses) will be collected, stored, or transferred by CubeBackup.
6. CubeBackup may collect the operating system, version number, and/or the license status information from our products running on the customer's machine. This information is logged to help diagnose technical problems and to constantly improve the quality of our products.

How is Google Workspace or Microsoft 365 data backed up and secured?

Our products back up Google Workspace or Microsoft 365 data using Google's and Microsoft's public APIs and strictly follow Google's and Microsoft 365's Developer Guide. We have implemented accepted standards of technology and operational security in order to protect backup data from loss, alteration or destruction. CubeBackup states that:

1. Google Workspace or Microsoft 365 data is downloaded by our products solely through Google or Microsoft APIs, including Google Workspace Admin SDK, Google Drive API, Gmail API, Google Contact API, Google Calendar API, Google Sites API or Microsoft Graph API.
2. Our products use Google domain-wide OAuth and Microsoft Azure AD application for authentication and authorization to protect customer's credentials. No Google Workspace or Microsoft 365 account passwords are required by our products.
3. All Google Workspace or Microsoft 365 data is transferred by our products using HTTPS protocol with Secure Socket Layer (SSL) data encryption to help ensure that data is secure and available only to our customers.
4. By default, backup data is AES encrypted on the customer's private storage. The private key for data encryption is also generated and stored on the customer's private storage. CubeBackup does not collect or store private encryption keys.
5. Permission controls, including Google Cloud Platform Project creation, Google Service account creation, Google Workspace domain authorization, Microsoft Azure AD application creation and authorization are left to our customers. The backup data and products running on our customer's machines are under the full control of our customers.
6. Customers can secure the product web console with Secure Socket Layer (SSL) encryption to help ensure that all communications between the desktop computer and the backup server are secure.

Cookies

CubeBackup's website uses cookies to facilitate and improve your experience of our website and CubeBackup has carefully chosen these cookies and have taken steps to ensure that your privacy and personal information are protected and respected at all times.

How does CubeBackup's website use cookies?

1. Before cookies are placed on your computer or device, you will be shown a pop-up requesting your consent to set those cookies. By giving your consent to the placing of cookies you are enabling us to provide the best possible experience and service to you. You may, if you wish, deny consent to the placing of cookies; however certain features of our site may not function fully or as intended.

2. When you submit data through a form, such as those found on contact pages or comment forms, cookies may be set to remember your user details for future correspondence.

3. We use cookies to track how you use our site by providing usage statistics on things such as how long you spend on the site and the pages that you visit.

4. Whilst this information on its own does not usually constitute your personal information, we may combine the information we collect by cookies with your personal information that we have collected from you in order to learn more about how you use the site, improve our services and continue to produce engaging content. A full list of cookies and how we use them can be found below in the section "cookies we use".

Cookies we use

The cookies we use or might use on our website are for **Performance/Analytical** purposes: These cookies allow us to collect certain information about how you navigate our site. They help us to understand which parts of our websites are interesting to you and which are not, as well as what we can do to improve them.

Cookies set by third-party sites

1. To enhance our content and to deliver a more enriching online experience for our users, we sometimes embed images and videos from other websites on the site.

2. You may be presented with cookies from third-party websites. Please note that we do not control the dissemination of these cookies and you should consult the relevant third party website for information on how these cookies are used and how you can control them.

3. This site may use Google Analytics cookies to help us to understand how you use the site and ways that we can improve your experience. For more information on Google Analytics cookies, see the official Google Analytics page.

Disabling cookies

1. Most internet browsers are initially set up to automatically accept cookies. Unless you have adjusted your browser settings to refuse cookies, our system will issue cookies when you direct your browser to our site.

2. You can refuse to accept cookies by activating the appropriate setting on your browser. Please be aware that restricting the use of cookies will impact the functionality of our site. As a result, you may be unable to access certain parts of our site or use some of our products and/or services.

3. Depending on your browser, further information may be obtained via the following links:

    - Firefox
    - Microsoft Edge
    - Google Chrome
    - Safari
    - Opera

Security Breach Response Procedure

Security Breaches are security violations in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. They may involve any kind of record, paper or electronic, and include the loss or theft of portable electronic media such as laptops or USB flash drives.

CubeBackup is committed to protecting CubeBackup's employees, partners, customers, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

When a security or privacy breach occurs, the response procedure must be followed as described below:

1. Immediately alert appropriate parties

Alert all relevant staff of the breach, including the security coordinator, and determine who else should be involved in addressing the breach. Information Custodians must provide the following information:

- the nature of the breach;
- the information that was exposed and approximate number of records concerned;
- to whom it was exposed;
- for how long it was exposed;
- likely consequences of the breach;
- measures taken or proposed to contain the breach; and
- the reason for delay for any report not made within 24 hours.

2. Notify those affected by the breach

Notify those affected in 48 hours if CubeBackup determines that the breach poses a real risk to individuals or organizations, taking into consideration the sensitivity of the information and whether it is likely to be misused. If law enforcement is involved, ensure that notification will not interfere with any investigations.

Notification should be direct, such as by telephone, letter, email or in person. Indirect notification can be used in situations where direct notification is not possible or reasonably practical, for instance, when contact information is unknown or the breach affects a large number of people.

Notification to affected individuals or customers should include:

- details of the extent of the breach and the specifics of the information that was compromised
- the steps taken and planned to address the breach, both immediate and long- term
- a suggestion, if financial information or information from government-issued documents is involved, to:

    a) contact their bank, credit card company, and appropriate government departments to advise them of the breach

    b) monitor and verify all bank account, credit card and other financial transaction statements for any suspicious activity

    c) obtain a copy of their credit report from a credit reporting bureau

- contact information for someone within CubeBackup who can provide additional information and assistance, and answer questions

3. Investigate

- Identify and analyze the events that led to the breach
- Review policies and practices in protecting information, privacy breach response plans and staff training to determine whether changes are needed
- Determine whether the breach was a result of a systemic issue and if so, review program-wide or institution-wide procedures
- Take corrective action to prevent similar breaches in the future and ensure all staff are adequately trained

GDPR

We have taken all necessary measures to ensure that our products and services fully comply with GDPR.

For more information regarding GDPR, please refer to our GDPR Compliance Statement.

Disclosure of data

CubeBackup may disclose your data in the good faith belief that such action is necessary to:

- To comply with a legal obligation.
- To protect and defend the rights or property of CubeBackup Inc.
- To prevent or investigate possible wrongdoing in connection with our Products and site.
- To protect against legal liability.

Children's Privacy

We are committed to protecting children's privacy. Our products and websites do not address anyone under the age of 18 ("Children"). We do not knowingly collect personally identifiable information from anyone under the age of 18. If you are a parent or guardian and you are aware that your child has provided us with personal data, please contact us. If we become aware that we have collected personal data from children without verification of parental consent, we will take steps to remove that information from our servers.

Links to other sites

Our site or products may contain links to other sites that are not operated by us. If you click on a third party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

Contact CubeBackup support

If you wish to submit a request to exercise your rights, under applicable privacy law, or have questions about how your information is handled at any time, or to make complaints, please contact our support team via support@cubebackup.com.

When requested, and provided that it is practical and commercially feasible to comply with the request, we will reply to your request within 15 days or such time as prescribed under application law.

Changes to this statement

We may update this Statement from time to time to comply with applicable law and regulations or other legitimate purposes. We may also separately advise you about the change. Subject to obtaining your explicit consent as may be required by applicable law, the new modified privacy will apply from that revision date. Therefore, we encourage you to review this Statement periodically to be informed about how we are protecting your information.