

## Vendor Statement of Compliance Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Animaker Inc ("Service Provider") on 01/14/2021 ("Effective Date").

**WHEREAS**, the LEA and the Service Provider entered into an agreement for Educational Technology services;

**WHEREAS**, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

**WHEREAS**, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

**NOW, THEREFORE**, the Parties agree as follows:

### Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

Agree: Yes  No

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

Agree: Yes  No

3. **PRIVACY.** The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

Agree: Yes  No

**Section I: General - All Data (Continued)**

4. **REUSE:** Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.  
Agree: Yes  No
5. **TRANSPORT:** Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.  
Agree: Yes  No
6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.  
Agree: Yes  No
7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?  
Agree: Yes  No
8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).  
Agree: Yes  No
9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.  
Agree: Yes  No

**Section II: AB1584 Compliance - Student Information Only**

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.  
Agree: Yes  No
2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.  
Agree: Yes  No
3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.  
Agree: Yes  No
4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.  
Agree: Yes  No
5. Vendor will attach to this document evidence how student data is kept secure and confidential.  
Agree: Yes  No
6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.  
Agree: Yes  No
7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).  
Agree: Yes  No
8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.  
Agree: Yes  No
9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students  
Agree: Yes  No

**Section III: SB 1177 SOPIPA Compliance - Student Information Only**

1. Vendors cannot target advertising on their website or any other website using information acquired from students.  
Agree: Yes  No
  
2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.  
Agree: Yes  No
  
3. Vendors cannot sell student information.  
Agree: Yes  No
  
4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.  
Agree: Yes  No
  
5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.  
Agree: Yes  No
  
6. Vendors must delete district-controlled student information when requested by the District.  
Agree: Yes  No
  
7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.  
Agree: Yes  No

As an authorized representative of my organization, I accept the conditions listed in this document.

**K. Loganathan**

Print Name

K. Loganathan  
Signature, Date

**Laura Assem, 01/14/2021**

Print Name (Roseville City School District)

Laura Assem  
Signature, Date (Roseville City School District)

## EXHIBITS

### Section II.5: Securing Student Data

Data in transit and rest is encrypted. We are using AWS KMS (Key Management Service) for all our keys.

The data connection to our application is encrypted and authenticated using a strong protocol (TLS 1.2), a strong key exchange (ECDHE\_RSA with P-256), and a strong cipher (AES\_128\_GCM). We use the SSL certificate signed by Go Daddy.

All symmetric key encrypt commands used within the HSA use the Advanced Encryption Standards (AES), in Galois Counter Mode (GCM) using 256-bit keys. The analogous calls to decrypt use the inverse function.

Amazon EC2 EBS volume is encrypted using AES-256-XTS. This requires two 256-bit volume keys, which is like a 512-bit volume key. The volume key is encrypted under a Customer Master Key and stored along with volume meta data.

### Section II.6: Disclosure Notification

Roseville City School District will be notified of a breach or any unauthorized disclosure within 72 hours after Animaker becomes aware of it.

### Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

Animaker will not collect any Personally Identifiable Information like Email ID, Date of Birth, age or Place from any of its user if they subscribe with us as a student user.

For other privacy policy of animaker, please refer to the below link,

<https://www.animaker.com/terms-policy>

### Section III.5: How Student Data is Protected:

Data in transit and rest is encrypted. We are using AWS KMS (Key Management Service) for all our keys.

The data connection to our application is encrypted and authenticated using a strong protocol (TLS 1.2), a strong key exchange (ECDHE\_RSA with P-256), and a strong cipher (AES\_128\_GCM). We use the SSL certificate signed by Go Daddy.

All symmetric key encrypt commands used within the HSA use the Advanced Encryption Standards (AES), in Galois Counter Mode (GCM) using 256-bit keys. The analogous calls to decrypt use the inverse function.

Amazon EC2 EBS volume is encrypted using AES-256-XTS. This requires two 256-bit volume keys, which is like a 512-bit volume key. The volume key is encrypted under a Customer Master Key and stored along with volume meta data.

## EXHIBITS

### Section 1.6: External Security

WAF.png and WAF-Realtime.png [attached] - Web Application Firewall which in place.

### Section 1.7: Internal Security

WAF.png and WAF-Realtime.png [attached] - Web Application Firewall which in place.

Animaker hosts all its customers' data only on AWS cloud and logically isolates each customer's data from that of other customers and users, even when its stored on the same physical server. Production data/systems are highly secured, and nobody possesses direct access to the system.

### Section II.2: Exporting of Student-Created Content

Animaker support the following formats like MP4, GIF, MP3, JPG for exporting the data (Media)

### Section II.4: Review and Correcting Personally Identifiable Information (PII)

Animaker will not collect any Personally Identifiable Informations like Email ID, Date of Birth, age or Place from any of its user if they subscribe with us as a student user.

For other privacy policy of animaker, please refer to the below link,

<https://www.animaker.com/terms-policy>



# Privacy Policy

## 1. INTRODUCTION

Our privacy policy (our “Privacy Policy”) will help you understand what information we collect at Animaker, how we use it, and what choices you have. We believe strongly that your personal information should be protected. We believe strongly in privacy. We will do what is necessary to protect your personal information and preserve its privacy.

When we talk about Animaker (“Animaker,” “we,” “our,” or “us”) in this Policy, we are referring to Animaker Inc., the company that provides the Services. When we talk about the “Services” in this Policy, we are referring to our online state of the art animation platform (the “Animaker Platform” or the “Platform”), sometimes known as the “Instance” and hosted services (“Animaker Services” or “Services”). When we talk about you (“you,” or “User”), we are talking about persons or entities, including your employer, who accesses or authorizes others to access our Platform, use our Services, download our mobile application (the “App”) and/or visit or register at our website ([www.animaker.com](http://www.animaker.com)) (our “Website”).



If you don't understand something in this Privacy Policy or our Terms of Service, please contact us at [legal@animaker.com](mailto:legal@animaker.com) and we will help you. Please do not register until you are comfortable with this Privacy Policy and our Terms of Service, which can be found here.

BUT NOTE, IF YOU ACCESS OUR PLATFORM, USE OUR SERVICES, DOWNLOAD OUR APP, REGISTER WITH US, OR NAVIGATE ON OUR WEBSITE, YOU AGREE TO COMPLY WITH AND BE BOUND BY THIS PRIVACY POLICY AND OUR TERMS OF SERVICE AT [HTTPS://WWW.ANIMAKER.COM/TERMS-POLICY](https://www.animaker.com/terms-policy). IF YOU DISAGREE WITH OR DO NOT WANT TO BE BOUND BY THIS PRIVACY POLICY, DO NOT ACCESS OUR PLATFORM, USE OUR SERVICES, DOWNLOAD OUR APP, REGISTER WITH US, OR NAVIGATE ON OUR WEBSITE.

Our Services are currently available for use via our Website or App specific to your desktop or mobile device, as further described in our Terms of Service at <https://www.animaker.com/terms-policy>. Unless not defined in this Privacy Policy, capitalized terms herein will have the same meaning as ascribed to them in our Terms of Service at <https://www.animaker.com/terms-policy>. One of our Services is commonly known as the "Instance," which enables users to easily create animations for use by their businesses.





## **2. INFORMATION WE COLLECT AND RECEIVE**

### **1. Customer Data**

Content and information submitted by you to register or access the Platform and/or use our Services are referred to in this Privacy Policy as “Customer Data.” Customer Data includes any information that describes you as an individual including name, email address, phone number, business address, title, IP address, employer, etc. In Europe such Customer Data is referred to as “Personal Data” and in the United States it is referred to as “Personally Identifiable Information” or “Personal Information.” Customer Data, Personal Data, Personal Information, and Personally Identifiable Information are used interchangeably in this Privacy Policy. Customer Data is controlled by the entity, usually an employer but sometimes an individual that is authorized to use the Platform (the “Customer”). Where Animaker collects or processes Customer Data, it does so on behalf of the Customer. Under the European Union’s Regulation (EU) 2016/679, General Data Protection Regulation (“GDPR”), you will be the “Controller,” as defined in the GDPR, of the Personal Data of your European employees and/or European residents or visitors, who access



our Platform on your behalf, and we will be the “Processor,” as defined in the GDPR, of such Personal Data.

If your Company authorizes you to join an Animaker-powered, customer-created Instance feature/function and create a user account, you are an “Authorized User,” as further described in the User Terms of Service at <https://www.animaker.com/terms-policy>. For sake of clarification, “you” or “your” generally refers to the Authorized User. If you are using the Services by invitation of a Customer, whether that Customer is your employer, another organization, or an individual, that Customer sets its own policies regarding storage, processing, access, modification, deletion, sharing, and retention of Customer Data, which may affect your use of the Services. Please check with the Customer about the policies and settings it has in place. In some cases, as fully discussed in our User Terms of Service at <https://www.animaker.com/terms-policy>, you may be both the Authorized User and the Customer.

## **2. Other information**

Animaker may also collect and receive the following information:

- a. Account creation information. Authorized Users may provide information such as an email address, phone number, and password to create an account.



b. Animaker Instance Setup Information. When a Customer creates an Animaker Instance using the Platform and our Services, we may collect an email address, name, photo, domain details (such as instance-name.Animaker.com), user name for the individual setting up the instance, and password. We may also collect administrative team contact info, such as a mailing address.

c. Billing and other information. For Customers that purchase a paid version of the Services, our corporate affiliates and our third-party payment processors may collect and store billing address and credit card information on our behalf or we may do this ourselves.

d. Services usage information. This is information about how you are accessing and using the Services, which may include administrative and support communications with us and information about the instances, channels, people, features, content, and links you interact with, and what third party content, assessments and integrations that you use (if any).

e. Contact information. With your permission, any contact information you choose to import is collected (such as an address book from a device) when using the Services.



f. Log data. When you use the Services our servers automatically record information, including information that your browser sends whenever you visit a website or your mobile application sends when you are using it. This log data may include your Internet Protocol address, the address of the web page you visited before using the Services, your browser type and settings, the date and time of your use of the Services, information about your browser configuration and plug-ins, language preferences, and cookie data.

g. Device information. We may collect information about the device you are using the Services on, including what type of device it is, what operating system you are using, device settings, application IDs, unique device identifiers, and crash data. Whether we collect some or all of this information often depends on what type of device you are using and its settings.

h. Geo-location information. Precise GPS location from mobile devices is collected only with your permission. WiFi and IP addresses received from your browser or device may be used to determine approximate location.

i. Services integrations. If, when using the Services, you integrate with a third party service, we will connect that service to ours. The third party



provider of the integration may share certain information about your account with Animaker.

j. Third party data. Animaker may also receive information from affiliates in our corporate group, our partners, or others that we use to make our own information better or more useful. This might be aggregate level information, such as which IP addresses go with which zip codes, or it might be more specific information, such as about how well an online marketing or email campaign performed.

## **3. OUR COOKIE POLICY**

### **1. Cookies (or browser cookies).**

A cookie is a small file placed on the hard drive of your computer. You may refuse to accept browser cookies by activating the appropriate setting on your browser. However, if you select this setting you may be unable to access certain parts of our website and/or mobile applications. Unless you have adjusted your browser setting so that it will refuse cookies, our system will issue cookies when you direct your browser to our website and/or mobile application.

### **2. Cookie Policy.**

Our cookie policy can be found



here

. Please read it.

### **3. Flash Cookies.**

Flash Cookies are local storage objects (or flash cookies) that collect and store information about your preferences and navigation to, from and on our website and/or mobile applications.

### **4. Web Beacons.**

Web beacons and similar technologies are small bits of code, which are embedded in web pages, ads, and e-mail, that communicate with third parties. We may use web beacons, for example, to count the number of users who have visited a particular web page, to deliver or communicate with cookies, and to understand usage patterns. We also may include web beacons in emails to understand whether messages have been opened, acted on, or forwarded.

### **5. Automatic Data Collection.**

We use automatic data collection to (a) understand and save your preferences for future visits; (b) compile aggregate data about website traffic and website interactions in order to offer better website



experiences and tools in the future; and (c) we may also use trusted third-party services that track this information on our behalf.

## **6. Advertising Networks.**

We may choose to work with Google AdWords, Doubleclick, AdRoll or other advertising networks. Each of these companies has its own privacy policy, which we encourage you to review. For more information about advertising and tracking online, visit the Network Advertising Initiative. This website allows consumers to “opt out” of the behavioral advertising delivered by member companies.

## **7. Personal Information.**

We do not collect personal information automatically, but we may tie this information to personal information about you that we collect from other sources or you provide to us.

# **4. HOW WE USE YOUR INFORMATION**

We use your information to provide and improve the Services.

## **1. Customer Data**

Animaker may access and use Customer Data as reasonably necessary and in accordance with User’s instructions to (a) provide, maintain and improve the Services and Instance; (b) to prevent or address service, security, technical issues or at a User’s request in



connection with customer support matters; (c) as required by law; and (d) as set forth in our agreement with the User or as expressly permitted in writing by the User.

## **2. Other information**

We use other kinds of information in providing the Services.

a. To understand and improve our Services. We carry out research and analyze trends to better understand how users are using the Services and improve them.

b. To communicate with you by:

i. Responding to your requests. If you contact us with a problem or question, we will use your information to respond.

ii. Sending emails and Animaker messages. We may send you Services and administrative emails and messages. We may also contact you to inform you about changes in our Services, our Service offerings, and important Service related notices, such as security and fraud notices. These emails and messages are considered part of the Services and you may not opt-out of them. In addition, we sometimes send emails about new product features or other news about Animaker. You can opt





out of these at any time by sending us an email at [info@Animaker.com](mailto:info@Animaker.com) or clicking at the unsubscribe button, where applicable.

iii. Billing and account management. We use account data to administer accounts and keep track of billing and payments.

iv. Communicating with you and marketing. We often need to contact you for invoicing, account management and similar reasons. We may also use your contact information for our own marketing or advertising purposes. You can opt out of these at any time by sending us an email at [info@Animaker.com](mailto:info@Animaker.com) or clicking at the unsubscribe button, where applicable.

v. Investigating and preventing bad stuff from happening. We work hard to keep the Services secure and to prevent abuse and fraud.

### **c. Disaggregated Data.**

This Privacy Policy is not intended to place any limits on what we do with data that is aggregated and/or de-identified so it is no longer associated with an identifiable user or Customer of the Services.

## **5. YOUR CHOICES**



## **1. Customer Data**

You provide us with instructions on what to do with your Customer Data. You have many choices and control over Customer Data. For example, you may provision or de-provision access to the Services, enable or disable third party integrations, manage permissions, retention and export settings, transfer or assign instances, share channels, or consolidate instances or channels with other instances or channels.

## **2. Other information**

If you have any questions about your information, our use of this information, or your rights when it comes to any of the foregoing, contact us at [Jerry@animaker.com](mailto:Jerry@animaker.com)

# **6. OTHER CHOICES**

## **1. Browser.**

In addition, the browser you use may provide you with the ability to control cookies or other types of local data storage. Your mobile device may provide you with choices around how and whether location or other data is collected and shared. Animaker does not control these choices, or default settings, which are offered by makers of your browser or mobile device operating system.



## **7. SHARING AND DISCLOSURE**

There are times when the information described in this Privacy Policy may be shared by Animaker. This section discusses only how Animaker may share such information. Customers determine their own policies for the sharing and disclosure of Customer Data. Animaker does not control how Customers or their third parties choose to share or disclose Customer Data.

### **1. Customer Data**

Animaker may share Customer Data in accordance with our agreement with the Customer and the Customer's instructions, including:

- a. With third party service providers and agents. We engage with third party companies or individuals to provide information and learning tools on Instance, therefore we share Customer Data with those third-party companies or individuals.
- b. With affiliates. We may engage affiliates in our corporate group to process Customer Data.
- c. With third party integrations. Animaker may, acting on our Customer's behalf, share Customer Data with the provider of an integration added by Customer. Animaker is not responsible for how the provider of an



integration may collect, use, and share Customer Data, as this is the responsibility of the Customer.

## **2. Other information**

Animaker may share other information as follows:

a. About you with the Customer. There may be times when you contact Animaker to help resolve an issue specific to an instance of which you are a member. In order to help resolve the issue and given our relationship with our Customer, we may share your concern with our Customer.

b. With third party service providers, content partners and agents. We may engage third party companies or individuals, such as third-party payment processors, to process information on our behalf. You may request a list of all of our third party subprocessors by email us at [legal@animaker.com](mailto:legal@animaker.com) or mail to our Mailing Address set forth below in subsection 4 of the International Users section.

c. With affiliates. We may engage affiliates in our corporate group to process other information.



### **3. Other types of disclosure**

Animaker may share or disclose Customer Data and other information as follows:

- a. During changes to our business structure. If we engage in a merger, acquisition, bankruptcy, dissolution, reorganization, sale of some or all of Animaker 's assets, financing, acquisition of all or a portion of our business, a similar transaction or proceeding, or steps in contemplation of such activities (e.g. due diligence).
- b. To comply with laws. To comply with legal or regulatory requirements and to respond to lawful requests, court orders and legal process.
- c. To enforce our rights, prevent fraud and for safety. To protect and defend the rights, property, or safety of us or third parties, including enforcing contracts or policies, or in connection with investigating and preventing fraud.
- d. We may disclose or use aggregate or de-identified information for any purpose. We may share aggregated or de-identified information with our partners or others for business or research purposes like telling a prospective Animaker Customer the average number of messages sent within a Animaker Instance in a day or partnering with research



firm or academics to explore interesting questions about learning science and knowledge management.

## **8. SECURITY**

### **1. Protection of Data.**

Animaker takes security seriously. We take various steps to protect information you provide to us from loss, misuse, and unauthorized access or disclosure. These steps take into account the sensitivity of the information we collect, process and store, and the current state of technology.

### **2. Security Measures.**

We have implemented measures designed to secure your personal information from accidental loss and from unauthorized access, use, alteration and disclosure. All information you provide to us is stored on secure servers of our hosting service provider partner.

### **3. Compliance with our Procedures.**

The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of website and/or mobile applications, you are



responsible for keeping this password confidential. We ask you not to share your password with anyone.

#### **4. Transmission via the Internet.**

Unfortunately, the transmission of information via the internet is not completely secure. Although we do our best to protect your personal information, we cannot guarantee the security of your personal information transmitted to our website and/or mobile applications. Any transmission of personal information is at your own risk. We are not responsible for circumvention of any privacy settings or security measures contained on the website and/or mobile applications.

## **9. YOUR CALIFORNIA PRIVACY RIGHTS**

We do not sell, trade, or otherwise transfer to third parties your personal information. California Civil Code Section § 1798.83 permits users of our website and/or mobile applications, who are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please send an email to [info@animaker.com](mailto:info@animaker.com)



## **10. CHILDREN'S INFORMATION**

Our Services are not directed to children under 13. We do not want any personal information about children under the age of 13. We will immediately delete such information when we learn of it. If you learn that a child under 13 has provided us with personal information without parental consent, please contact us at [info@animaker.com](mailto:info@animaker.com)

## **11. INTERNATIONAL USERS**

### **1. Processing Data in the US.**

We are headquartered in the United States. Most of operations are located in the United States and India. Your Personal Data, which you give to us during registration or use of our Platform, may be accessed by or transferred to us in the United States. If you are visiting our web site or registering for our Services from outside the United States, be aware that your Personal Information may be transferred to, stored, and processed in the United States. Our servers or our third-party hosting services partners are located in the United States. By using our site, you consent to any transfer of your Personal Data out of Europe for processing in the US or other countries. If you are resident, employee, or visitor in Europe, the processing, storage, transfer, and use of your Personal Data may be subject to the rules and regulations of the GDPR.





## **2. EU-US and SWISS-US Privacy Shield Certification.**

We are currently in the process of self-certifying under the EU-US Privacy Shield and the SWISS - US Privacy Shield Certification (collectively the “Privacy Shield Certification”) with the U.S. Department of Commerce. We will let you know when we have obtained such Privacy Shield Certification.

## **3. Standard Contractual Clauses.**

Until we obtain such Privacy Shield Certification, we will comply with the EU Standard Contractual Clauses with respect to the transfer of Personal Data from the EU to the US and other countries for processing. If there is any conflict between the terms and conditions in this Privacy Policy and your rights under the EU Standard Contractual Clauses, the terms and conditions in the EU Standard Contractual Clauses will govern. For the purposes of this Privacy Policy, “EU Standard Contractual Clauses” mean the standard contractual clauses for the transfer of personal data to processors established in third countries (Commission Decision 2010/87/EC).

## **4. Sharing Personal Data with Third Parties.**

We do not (i) share such Personal Data with third parties, other than Processors or Sub-Processor (collectively “Agents”), who comply with GDPR and are required by us to provide our Services under our Terms of Service or an agreement with Customers under which we provide our



Services, or (ii) utilize any Personal Data for reasons other than that for which it was originally provided. If this practice should change in the future, we will update this Privacy Policy to identify any third parties and provide you with opt-out or opt-in choice where applicable. We are committed to resolving complaints about your privacy and our collection, storage, processing or use of your personal information transferred to the United States pursuant to Privacy Shield quickly and expeditiously. You should submit inquiries or complaints to us at [legal@animaker.com](mailto:legal@animaker.com) or at our mailing address: Animaker Inc.

3260 Hillview Avenue,  
Palo Alto, CA 94304, USA  
Attn: Privacy Coordinator

## **12. GDPR: FOR OUR EUROPEAN VISITORS, CONSUMERS, AND CUSTOMERS**

If you are a resident of or a visitor to Europe, you have certain rights with respect to the processing of your Personal Data, as defined in the GDPR.

Please note that in some circumstances, we may not be able to fully comply with your requests, or we may ask you to provide us with



additional information in connection with your request, which may be Personal Data, for example, if we need to verify your identity or the nature of your request.

In such situations, however, we will still respond to let you know of our decision. As used herein, “Personal Data” means any information that identifies you as an individual, such as name, address, email address, IP address, phone number, business address, business title, business email address, company, etc.

To make any of the following requests, contact us using the contact details referred to in the “Contact Information” section of this Policy.

### **1. Access:**

You can request more information about the Personal Data we hold about you. You can also request a copy of the Personal Data.

### **2. Rectification:**

If you believe that any Personal Data we are holding about you is incorrect or incomplete, you can request that we correct or supplement such data. You can also correct some of this information directly by logging into your service account. Please contact us as soon as possible upon noticing any such inaccuracy or incompleteness.



### **3. Objection:**

You can contact us to let us know that you object to the collection or use of your Personal Data for certain purposes.

### **4. Erasure:**

You can request that we erase some or all of your Personal Data from our systems.

### **5. Restriction of Processing:**

You can ask us to restrict further processing of your Personal Data.

### **6. Portability:**

You have the right to ask for a copy of your Personal Data in a machine-readable format. You can also request that we transmit the data to another entity where technically feasible.

### **7. Withdrawal of Consent:**

If we are processing your Personal Data based on your consent (as indicated at the time of collection of such data), you have the right to withdraw your consent at any time. Please note, however, that if you exercise this right, it may limit your ability to use some/ all of our Services or Platform and you may have to then provide express consent on a case-by-case basis for the use or disclosure of certain of your



Personal Data, if such use or disclosure is necessary to enable you to utilize some or all of our Services and Platform.

### **8. Right to File Complaint:**

You have the right to lodge a complaint about our practices with respect to your Personal Data with the supervisory authority of your country or EU Member State. Please go to [https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index\\_en.htm](https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm) to locate your Data Protection Authority.

## **13 CHANGES TO OUR PRIVACY POLICY**

It is our policy to post any changes we make to our privacy policy on this page. If we make material changes to how we treat our users' Personal Data, we will notify you by e-mail to the e-mail address specified in your account and/or through a notice on the Site home page and comparable place on the App. The date the privacy policy was last revised is identified at the top of the page. You are responsible for ensuring we have an up-to-date active and deliverable e-mail address for you, and for periodically visiting our Site and/or App and this privacy policy to check for any changes.



## **14. COPYRIGHT INFRINGEMENT / DMCA NOTICE**

If you believe that any content on our Website or App violates your copyright, and you wish to have the allegedly infringing material removed, the following information in the form of a written notification (pursuant to the Digital Millennium Copyright Act of 1998 (“DMCA Takedown Notice”)) must be provided to our designated Copyright Agent.

1. Your physical or electronic signature;
2. Identification of the copyrighted work(s) that you claim to have been infringed;
3. Identification of the material on our Website that you claim is infringing and that you request us to remove;
4. Sufficient information to permit us to locate such material;
5. Your address, telephone number, and e-mail address;



6. A statement that you have a good faith belief that use of the objectionable material is not authorized by the copyright owner, its agent, or under the law; and

7. A statement that the information in the notification is accurate, and under penalty of perjury, that you are either the owner of the copyright that has allegedly been infringed or that you are authorized to act on behalf of the copyright owner.

Animaker's Copyright Agent to receive DMCA Takedown Notices is Loganathan Kodiyarasu, at [logu@animaker.com](mailto:logu@animaker.com), Animaker Inc., Attn: DMCA Notice, 3260 Hillview Avenue, Palo Alto, CA 94304, United States of America. You acknowledge that for us to be authorized to take down any content, your DMCA Takedown Notice must comply with all the requirements of this Section. Please note that, pursuant to 17 U.S.C. § 512(f), any misrepresentation of material fact (falsities) in a written notification automatically subjects the complaining party to liability for any damages, costs and attorneys' fees incurred by Animaker in connection with the written notification and allegation of copyright infringement.

## **15. CALIFORNIA CONSUMER PRIVACY ACT**



For our California visitors and consumers: This Section supplements the information contained in our Privacy Policy above and applies solely to all visitors, users, and others to our website, who reside in the State of California (“consumers” or “you”). We adopt this Section to comply with the California Consumer Privacy Act of 2018 (“CCPA”), which becomes effective on January 1, 2020, and any terms defined in the CCPA have the same meaning when used in this Section.

### **1. Right to Request Personal Information.**

Upon request, we will provide you with (i) a list of all Personal Information that we have collected on you, (ii) from whom we obtained such Personal Information, (iii) the reason why we collected such Personal Information, and (iv) with whom (if any) we have shared such Personal Information. If we sell your Personal Information or disclose your Personal Information to third parties, upon request, we will provide you with (i) a list of the Personal Information that we have collected on you, (ii) a list of the Personal Information that we sell or disclose to others on you, and (iii) to whom we have sold or disclosed your Personal Information. A consumer can make such a request only twice in a 12-month period. We require such Personal Information to be able to provide to you our Services. Unless otherwise specified, we only collect Personal Information from you. We do not use others to provide us with your Personal Information.





## **2. Disclosure of Personal Information.**

We only share your Personal Information with service providers, e.g., billing and collection agents, who enable us to provide our Services to you. We do not sell or give your Personal Information to third parties for purposes unrelated to our provision of Services to you.

## **3. Right to have Personal Information Deleted.**

Upon request, we will delete all of your Personal Information that we have collected on you and will direct our Service Providers to also delete all of your Personal Information. But note that if we do delete all of this Personal Information, you will no longer be able to use our Services.

## **4. Non-Discrimination Right.**

We will not discriminate against you for exercising any of your CCPA rights. Unless permitted by the CCPA, we will not:

- a. Deny you goods or services.
- b. Charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties.
- c. Provide you a different level or quality of goods or services.



d. Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

## **5. Financial Incentives.**

However, we may offer you certain financial incentives permitted by the CCPA that can result in different prices, rates, or quality levels. Any CCPA-permitted financial incentive we offer will reasonably relate to your personal information's value and contain written terms that describe the program's material aspects. Participation in a financial incentive program requires your prior opt in consent, which you may revoke at any time.

## **6. Contact Information.**

You may contact us (i) at [legal@animaker.com](mailto:legal@animaker.com) (ii) by phone at our toll-free number +1 888-359-9292 , or (iii) by writing to us at Privacy Officer, at Animaker Inc., 3260 Hillview Avenue, Palo Alto, CA 94304, USA to (i) make a Personal Information Request, (ii) lodge a complaint about our use or storage of your Personal Information, (iii) ask us to delete such Personal Information, and/or (iv) discuss our Privacy Policy and/or anything that has to do with it. We will respond within forty-five (45) days of receiving such request or query. Additionally, in order for us to respond to your request or query, we will need to collect information from the requesting party to verify their identity.



## **7. Under 16.**

We will not sell your Personal Information if you are under the age of 16 unless we have the consent of your parent or your guardian nor will we sell it if you ask us not to do so.

## **8. Opt Out Right.**

Upon your request, we will stop selling your Personal Information (sometimes called your Opt Out Right). You may send the request to Opt Out (i) to [legal@animaker.com](mailto:legal@animaker.com), (ii) by phone at our toll-free number +1 888-359-9292 , or (iii) by writing to us at Privacy Officer, Animaker Inc., 3260 Hillview Avenue, Palo Alto, CA 94304, USA

## **9. Personal Information that We Store.**

For your information, we store/collect the following Personal Information on you:

Name

Business Address

Business Email Address

Business Telephone Number



IP Address

Business Title

Employer

### **10. Personal Information.**

We do not want you to enter your personal home address, your personal email, or any other “personal” information.

## **16. CONTACTING US**

If Users, Customers and/or Consumers have any questions, concerns, or complaints about our Privacy Policy, the Privacy Shield Certification, or how we process your Personal Data, please email us at [legal@animaker.com](mailto:legal@animaker.com) or send a letter to the following person:

Name: Jothimani R

Title: DevOps Engineer/Privacy Shield Organization

Contact Address: Company: Animaker Inc, 3260, Hillview Avenue, Palo Alto, California 94304



Email Address: [jothimani@animaker.com](mailto:jothimani@animaker.com)

Users, Customers, and/or Consumers may also contact our corporate officer, who is overall responsible for privacy at Animaker, if you have any questions about our Privacy Policy, Privacy Shield Certification, or Terms of Use:



- Name: Loganathan Kodiyarasu
- Title: Chief Operating Officer/Privacy Shield Organization Corporate Officer
- Company: Animaker, Inc.
- Address: 3260, Hillview Avenue, Palo Alto, California 94304
- Email: logu@animaker.com
- Phone: +1 888-359-9292

Under custom privacy policy signing with Deloitte, We are confirming the above policies will be applicable for all Deloitte's Animaker website users irrespective of their countries.

**ANIMAKER, INC.**

By: *K. Loganathan*

Name: Loganathan K  
Title: CISO



# Animaker - Data Encryption Standards

January 2020



## Overview

This document describes the overview of the encryption solution which was in place across Animaker AWS environment and the type of technology used to achieve the same

Animaker KMS provides centralized control over the lifecycle and permissions of your keys. Create new keys whenever you wish, and you can control who can manage keys versus who can use them.

## Solutions with Encryption enabled:

- S3
- EC2
- RDS
- Elastic Search
- Underlying EBS volumes





## Compliance

Security and quality controls in KMS have been validated and certified by the following compliance regimes:

- PCI DSS Level 1
- FIPS 140-2.
- FedRAMP.
- HIPAA.

## Screenshot of KMS solution dashboard

Alias	Key ID	Status
aws/elasticache	[Redacted]	Enabled
aws/ebs	[Redacted]	Enabled
aws/es	[Redacted]	Enabled
aws/elasticsearch	[Redacted]	Enabled
aws/backup	[Redacted]	Enabled
aws/redshift	[Redacted]	Enabled
aws/s3	[Redacted]	Enabled
aws/lambda	[Redacted]	Enabled
aws/rds	[Redacted]	Enabled
aws/iam	[Redacted]	Enabled