Privacy Policy

Last Updated: April 21st, 2020

WE CREATED THIS PRIVACY POLICY BECAUSE WE HIGHLY VALUE YOUR PERSONAL DATA AND INFORMATION.

PLEASE READ IT AS IT INCLUDES IMPORTANT INFORMATION REGARDING YOUR PERSONAL DATA AND INFORMATION.

1. Privacy Statement

AllCloud Inc. and subsidiaries of AllCloud BSD Ltd., AllCloud Platforms Ltd., AllCloud Business Applications Ltd., AllCloud (RO), AllCloud (DE), AllCloud USA LLC (US) and AllCloud ULC (CA) (all together hereinafter: "AllCloud" and/or "We") are leading global Cloud Solutions Providers with expertise across the cloud stack, infrastructure, Platform, and Software-as-a-Service. AllCloud headquarters are based in Israel.

AllCloud provides cloud consulting, cloud management and reselling services (all together hereinafter: "**The Services**"). AllCloud develops and operates AllCloud's Website: www.allcloud.io (hereinafter: "The Website").

THIS PRIVACY POLICY REFERS TO THE SERVICES AND THE WEBSITE, ALLCLOUD'S CUSTOMERS OR POTENTIAL CUSTOMERS, CUSTOMERS' END-USERS, ALLCLOUD'S EMPLOYEES AND SERVICE PROVIDERS, AND THE USERS OF THE WEBSITE.

This Privacy Policy sets forth our policy with respect to:

- Information that can be associated with or which relates to a person and/or could be used to identify a person, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, all as defined by the General Data Protection Regulation (GDPR) (EU) 2016/679 (**"Personal Data"**).

- As it refers to California's consumers or individuals where their data is collected in the state of California, this Privacy Policy sets forth our policy with respect to Information,
  - that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or California household such as a real name, alias, postal address, unique personal identifier, online identifier, Internet

Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers; and /or

- that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, their name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

All as defined by the California Consumer Privacy Act of 2018 (**"CCPA"**).

"Non-Personal Data," as used in this Privacy Policy, is therefore any information that does not relate to a person, cannot be used to identify a person, and/or refers to information collected in the state of California Publicly Available Information.

We may also use Non-Personal Data. The limitations and requirements in this Privacy Policy on how we gather, use, disclose, transfer, and store/retain Personal Data do not apply to Non-Personal Data.

2. Data that we use, receive, collect, process, share, or store and how we use it

2.1. **Information relating to Customers or Potential Customers, Service Providers, Employees or Candidates, Service Users, etc.:**

2.1.1. AllCloud uses, receives, collects, processes or stores only that Information which is necessary to provide its services and operate its business.

We might use, receive, collect, process or store Information on potential customers, customers, employees, service providers, users of the Website etc. This Information may include Personal data such as:

Name, phone, email address, personal/physical address, representative personal contact details, phone and cellphone numbers financial information (i.e. billing information, bank account information, credit card information), VAT Number, signature, end users' website engagement and usage data, IP address, audio, electronic, visual and similar information, such as images and audio, video or call recordings created in connection with our business activities, social network contact accounts, employee's health information, employee's biometric information (i.e. fingerprint), employee's and candidate CVs, employees Social security number/ID number/passport number , employee's health insurance

information, employee's education and employment history, etc. We use cookies and similar tracking technologies to track the activity on our Website and hold certain information. Cookies are files with a small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Tracking technologies also used are beacons, tags, and scripts to collect and track information and to improve and analyze our Website and services. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Website. Examples of cookies we use:

- Session cookies – for operating our Websites
- Preference cookies – for remembering your preferences and various settings
- Security cookies – for security purposes

We obtain the categories of personal information listed above from the following categories of sources:

- Directly from our clients or their agents. For example, from information our clients provide to us related to the Services for which they engage us.
- Directly from you. For example, through information we ask from you when our clients or their agents engage our Services.
- Directly and indirectly from you when using our Services or visiting our website. For example, usage details collected automatically during your interaction with our website.

2.1.2. This Information provided to us voluntarily and/or through the data owner's consent to collect and process it, and/or the processing thereof is necessary to meet contractual obligations entered into by the data owner and AllCloud, and/or the processing thereof is necessary for AllCloud to comply with its legal obligations, and/or the processing thereof is for the purposes of legitimate interests pursued by AllCloud.

2.1.3. **We use this Personal Data in a manner that is consistent with this Privacy Policy and applicable laws and regulations. We may use the Personal Data as follows:**

2.1.3.1. **Processing and Analyzing:** In order to provide AllCloud's services and operate its business, AllCloud may use the Personal Data for processing and analyzing purposes.

2.1.3.2. **Specific Purpose:** If you provide Personal Data for a specific purpose, AllCloud may use said Personal Data in connection with the purpose for which it was provided. For instance, if you contact AllCloud by email, we will use the Personal Data you provide to

answer your question or resolve your problem and will respond to the email address used to contact us.

2.1.3.3. **Internal Business:** We may use your Personal Data for internal business purposes, including, without limitation, to help us improve Website content and functionality to better understand our Customers and Users, to improve our Services, to protect against, identify or address wrongdoing, to enforce our Contracts and this Privacy Policy, to provide you with customer service, and to generally manage and operate our business (e.g., pay salaries, etc.).

2.1.3.4. **Marketing:** We may use any Personal Data you provide us with to contact you in the future for our marketing and advertising purposes, including, without limitation, to inform you about new services we believe might be of interest to you, and to develop promotional or marketing materials and provide those materials to you. IF YOU RECEIVE DIRECT MARKETING BY MISTAKE OR WITHOUT YOUR SPECIFIC CONSENT AND/OR YOU WISH TO OPT-OUT, YOU ARE REQUIRED TO CONTACT US AT dpo@allcloud.io.

2.1.3.5. **Statistics:** We may use any Personal Data you provide us with to generate statistical reports containing aggregated information.

2.1.3.6. **Security and Dispute Resolution:** We may use Personal Data to protect the security of our Website and Services, to detect and prevent cyberattacks, fraud, phishing, identity theft, and data leaks, to verify genuine software licenses, to resolve disputes, and to enforce our agreements.

2.1.3.7. **Data Retention, Archives:** We retain and archive Personal Data so long as it is necessary to operate our business and maintain our Services, meet contractual obligations, laws and regulations, and are subject to our retention policies and this Privacy Policy.

2.1.3.8. **Transfer/Share/Disclose Data:** We may share your Personal Data with our Partner, contractors and service providers who process Personal Data on behalf of the Company to perform certain business-related functions. We may provide them with information, including Personal Data, in connection with their performance of such functions. While we do so, we make sure that they are bound to maintain said Personal Data in accordance with this Privacy Policy. When we disclose the Personal Data, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract. In

the preceding twelve (12) months, we have disclosed the above said categories of Personal Data.

2.1.3.9. **Cloud Services:** We may need to share Personal Data with our cloud service. For example, to assist in protecting and securing our Website or Services the cloud service admin may need access to Personal Data to provide those functions. In such cases, the cloud service provider must abide by our data privacy and security requirements and is not allowed to use Personal Data they receive from us for any other purpose.

2.1.3.10. **Development and Customer Service:** For example, to provide customer service and support or assist in protecting and securing our systems and services our development and customer service team may require access to Personal Data. In such cases, our personnel must abide by our data privacy and security requirements and policy and are not allowed to use Personal Data for any other purpose.

2.1.3.11. **Corporate Sale, Merger, Reorganization, Dissolution or Similar Event**: Personal Data may be part of the transferred assets. You acknowledge and agree that any successor to or acquirer of AllCloud (or its assets) will continue to have the right to use your Personal Data and other information in accordance with the terms of this Privacy Policy.

2.1.3.12. **Law Enforcement:** In order to, for example, respond to a subpoena or request from law enforcement, a court or a government agency (including in response to public authorities to meet national security or law enforcement requirements), or in the good faith belief that such action is necessary to (a) comply with a legal obligation, (b) protect or defend our rights, interests or property or that of third parties, (c) prevent or investigate possible wrongdoing in connection with the Services, (d) act in urgent circumstances to protect the personal safety of Users of the Website and Services or the public, or (e) protect against legal liability.

2.1.3.13. **Other Purposes:** If we intend to use any Personal Data in any manner not consistent with this Privacy Policy, you will be informed of such anticipated use prior to or at the time the Personal Data is processed.

2.1.3.14. We are not selling Personal Data to third parties.

IF YOU HAVE A REASONABLE BASIS TO ASSUME OR YOU KNOW THAT ANY OF THE ABOVE MENTIONED IS NOT MET, YOU ARE REQUIRED TO PROMPTLY INFORM US, WITHOUT DELAY, BY SENDING US AN EMAIL TO: dpo@allcloud.io.

2.2. Non-Personal Data: Since Non-Personal Data cannot be used to identify you in person, we may use such data in any way permitted by law

3. How We Store and Transfer Information

3.1. In order to provide our Services, manage and operate our business, we use third parties cloud services such as:

3.1.1. Amazon Cloud Services which comply with the GDPR and is ISO 27001, 27017,27018 certified (for AWS full statement see https://aws.amazon.com/blogs/security/all-aws-services-gdpr-ready/). AllCloud stores some of its Information, which may contain Personal Data, at AWS cloud services in Ireland region (eu-west-1).

3.1.2. Google's G-suite services & Google Cloud Platform which are committed to GDPR compliance. (For Google Cloud full statement see https://cloud.google.com/security/gdpr/) .

3.1.3. Salesforce cloud services which will comply with the GDPR in the delivery of their services, certify compliance with the EU-U.S. Privacy Shield Framework and is ISO 27001, 27017,27018 certified (for a Salesforce full statement see https://www.salesforce.com/eu/campaign/gdpr/).

3.2. In order to deliver our services and/or operate our business, Information, which may include Personal Data, may be processed by our third parties service providers ("Suppliers"). We transfer only the minimum data that is necessary for conducting our services. The data is transferred only to suppliers approved by us that allow compliance with GDPR.

3.3. Personal data may be transferred, stored, and processed in countries outside the EU or European Economic Area (EEA). Such a transfer to third countries may include countries that do not ensure an adequate level of data protection as required by EU privacy laws. We implement high levels of information security techniques & technical measures and/or third parties' contractual obligations to maintain their Information security level adequate to the AllCloud level.

3.4. We may transfer Personal data to the country of Israel where we maintain our headquarter facilities. Israel is considered by the EU as having adequate data protection laws.

3.5. See our Privacy Shield statements (section 6 and 7 below) for information on our practices with regard to data transferred from the EU to AllCloud USA LLC.

AllCloud

4. Personal Data Security

4.1. We are strongly committed to protecting your Personal Data and information, and we will take reasonable technical steps, accepted in our industry, to keep your Information secure and protect it against loss, misuse or modification. However, no network, server, database or email transmission is ever fully secure or error-free. Therefore, you should take special care in deciding what information you disclose.

4.2. If you notice any security risks or violations, we advise you to report them to us at dpo@allcloud.io so that we may resolve them as soon as possible.

4.3. We recommend that you use, disclose and share your Personal Data and information with caution and do not give out Personal Data and information unless it is necessary, as we cannot guarantee the security of data over the internet and cannot control the actions of other users of the Services with whom you choose to share Personal Data and information.

4.4. AllCloud implements legal, technical and organizational information security measures based on the ISO certification mechanisms specified in ISO 27001:2013 – Information Security Management Systems, ISO 27017:2015 – Information Security Controls for Cloud Services, and ISO 27018:2014 – Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors. AllCloud is ISO 27001, 27017 certified.

5. Individual/California Consumer rights: Accessing, Updating, Correcting, and Deleting Information, Restricting Information Processing.

5.1. You may have the **right to request access** to some of your Personal Data being stored by us. California consumers (California residents) have the right to request that we disclose certain information to them about our collection and use of their personal information over the past 12 months.

Once we receive and confirm your verifiable consumer or individual request, we will disclose to you, inter alia:

- The categories of personal information we collected about you
- Our business or commercial purpose for collecting that personal information
- The categories of third parties with whom we share that personal information

- The specific pieces of personal information we collected about you (also called a data portability request)

5.2. You can also request to **correct and update any inaccurate Personal Data or ask to delete Personal Data** that we process about you. The foregoing is subject to our policies and the applicable laws and regulations. Once we receive and confirm your verifiable consumer/individual request, we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

5.2.1. According to the CCPA, we may deny California consumer's deletion request if retaining the information is necessary for us or our service providers to:

- Complete the transaction for which we collected the personal information, provide our services that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- Debug products to identify and repair errors that impair existing intended functionality.
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 seq.).
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.
- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
- Comply with a legal obligation.
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

5.3. In order **to exercise these rights**, you can contact us at: dpo@allcloud.io or call us at: 1-800 416-8949 (Toll free number) Only you or other person that you authorize to act on your behalf , California resident or a person registered with the California Secretary of State that California resident authorize to act on its behalf, may make a verifiable individual or consumer request related to their Personal Data. California residents may only make a verifiable consumer request for access or data portability twice within a 12-month period.

5.3.1. The verifiable consumer or individual request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.
- **We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you**. We will only use personal information provided in a verifiable consumer/Individual request to verify the requestor's identity or authority to make the request.

5.3.2. **Response Timing and Format.** We endeavor to respond to a verifiable consumer request within 45 days (by the CCPA) or 30 days (By the GDPR) of its receipt. If we require more time, we will inform you of the reason and extension period in writing. We will deliver our written response via email. For California residents, any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily usable and should allow you to transmit the information from one entity to another entity without hindrance.

5.3.3. We do not charge a fee to process or respond to your verifiable consumer or Individual request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

5.4. **Non-Discrimination**. We will not discriminate against you for exercising any of your CCPA or GDPR rights. Unless permitted by the CCPA and GDPR, we will not: Deny you use of our Services and /or Provide you a different level or quality of Services.

5.5. We may **retain** your Personal Data for any period permitted or required under applicable laws. Even if we delete your Personal Data it may remain stored on backup or archival media for an additional period of time due to technical issues or for legal, tax or regulatory reasons, or for legitimate and lawful business purposes.

5.6. You may have the right to restrict processing if one of the following applies:

5.6.1. The accuracy of the Personal Data is contested by the data owner;

5.6.2. The processing is unlawful and the data owner objects to having their Personal Data erased, instead requesting that its use be restricted;

5.6.3. Your service provider no longer needs the Personal Data for the purposes of the original processing, but the data is required by the data owner for establishing, exercising or defending legal claims;

5.6.4. The data owner has objected to processing pending verification of whether the legitimate grounds of your service provider override those of the data owner.

If you wish to **object to processing**, you are required to contact us at dpo@allcloud.io.

6. EU-U.S. Privacy Shield Framework

6.1. AllCloud USA LLC complies with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries transferred to the United States pursuant to Privacy Shield. AllCloud USA LLC has certified that it adheres to the Privacy Shield Principles with respect to such data. If there is any conflict between the policies in this privacy policy and data subject rights under the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/

6.2. **The types of data** that we process and may be governed under the EU-US Privacy shield are Personal Data related to our business Customers/prospects such as: name, phone, email address, personal address, representative personal contact details, financial information (i.e. billing

information, bank account information, credit card information), social network contact accounts, etc.

6.3. We collect, store and use that data **for the purpose** of providing our services and operating our business. For example, we may use your contact details for sales, marketing, support, billing etc.

6.4. **Your rights to access, to limit use, and to limit disclosure:** EU individuals have rights to access personal data about them, and to limit use and disclosure of their personal data. With our Privacy Shield self-certification, AllCloud has committed to respect those rights. If you wish to request access, to limit use, or to limit disclosure, you are welcome to contact us by email at dpo@allcloud.io. We will provide an individual opt-out choice, or opt-in for sensitive data, before we share your data with third parties other than our agents, or before we use it for a purpose other than which it was originally collected or subsequently authorized. To request to limit the use and disclosure of your personal information, please submit a written request to dpo@allcloud.io.

6.5. We may use third parties' services or transfer data to our affiliate's companies, business partners, advertisers, vendors etc. all for the purpose of providing our services and operating our business. A list of specific third parties and how we secure the transferred data can be found at sections 3&4 above. AllCloud USA LLC's accountability for personal data that it receives in the United States under the Privacy Shield and subsequently transfers to a third party is described in the Privacy Shield Principles. In particular, AllCloud USA LLC remains responsible and liable under the Privacy Shield Principles if third-party agents that it engages to process the personal data on its behalf do so in a manner inconsistent with the Principles, unless AllCloud USA LLC proves that it is not responsible for the event giving rise to the damage.

6.6. **U.S. Federal Trade Commission enforcement:** Our commitment under the Privacy Shield are subject to the investigatory and enforcement powers of the United States Federal Trade Commission.

6.7. **Compelled disclosure:** We may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

7. Inquiries and complaints under the Privacy Shield:

7.1. In compliance with the Privacy Shield Principles, AllCloud USA LLC commits to resolve complaints about your privacy and our collection or use of your personal information transferred to the United States pursuant to Privacy Shield. European Union individuals with Privacy Shield

inquiries or complaints should first contact AllCloud USA LLC at: dpo@allcloud.io. We will respond within 45 days.

7.2. AllCloud USA LLC has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgement of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbb.org/EU-privacy-shield/for-eu-consumers for more information and to file a complaint. This service is provided free of charge to you.

7.3. If your Privacy Shield complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Privacy Shield Annex 1 at https://www.privacyshield.gov/article?id=ANNEX-I-introduction.

8. General

8.1. This Privacy Policy does not apply to any Personal Data that you provide to third-parties.

8.2. This Privacy Policy applies only to the Services and Website; it does not apply to third-party websites or services linked to by the Website or whose services we distribute. Links from the Website or the distributed third-parties' services do not imply that we endorse or have reviewed said third-party websites or services. We suggest contacting these third-parties directly for information regarding their privacy policies.

9. Change in Terms and Conditions

The Services and our business may change from time to time. As a result, at times it may be necessary for us to make changes to this Privacy Policy. We reserve the right, at our sole discretion, to update or modify this Privacy Policy at any time (collectively, "Modifications"). Modifications to this Privacy Policy will be posted on the Website with a revised 'Last Updated' date at the top of this Privacy Policy.

Please review this Privacy Policy periodically, and especially before you provide any Personal Data or information. This Privacy Policy was last updated on the date indicated above. Your continued use of the Services following the implementation of any Modifications to this Privacy Policy constitutes acceptance of those Modifications. If you do not accept any Modification to this Privacy Policy, your sole remedy is to cease accessing, browsing and otherwise using the Website or our Services.

10. Dispute Resolution

10.1. If you have a complaint about AllCloud's privacy practices, you should write to us at: dpo@allcloud.io.

Our Contact details:

ISRAEL (HEADQUARTERS)	GERMANY (MUNICH)	ROMANIA	USA
Contact Person: Admit Ivgi, DPO	Contact Person: Uli Baur	Contact Person: Diana Teashala	Contact Person: Douglas Shepard
Address: 13 Amal St., Building A, 2nd Floor. POB: 11390 Rosh Haayin, 4809280 Tel: +972 (3) 6783868 Fax: +972 (3) 5048647	Address: Rechtsanwaltsgesellschaft mbH Prinzregentenstr. 78 Munich, 81675 Germany Tel: +49 172 295 295 1	Address: Strada George Enescu 23 București, 010303 Romania	Address: 155 Montgomery, Suite # 810 San Francisco 94104 California, USA Tel: +1 415 549 0861

10.2. We will take reasonable steps to work with you to attempt to resolve your complaint.

11. General Inquiries and Complaints

11.1. You may have the right to lodge a complaint with a supervisory authority. However, prior to doing so, you are welcome to contact us by email at dpo@allcloud.io in order to resolve the issue for the benefit of all parties.

11.2. Our supervisory authorities are the Israeli, Germany and Romanian Data Protection authorities. Contact information for EU Supervisory Authorities is available here: https://edpb.europa.eu/about-edpb/board/members_en.