

Privacy Policy

[ISMS - A.5.34]

Document Properties

Internal ID:	20241106005
Revision:	3.0
Date of revision:	August 4, 2025
Confidentiality Level:	Public
Pages:	15

Change & Revision History

Rev.	Version Date	Description of Changes	Updated By
1.0	01.01.2019	Initial Policy Draft	Admit Ivgi
1.1	19.01.2021	Confirmation of document validity	Richard Lockson
2.0	11.05.2021	Update document	Admit Ivgi, CO
2.0	24/05/2022	Reviewed	Elisa P Kassahun, Compliance Officer
2.0	February 14 2023	Reviewed	Elisa P Kassahun, Compliance officer
2.1	December 26, 2023	New Template	Elisa P Kassahun, Compliance officer
3.0	January 3, 2024	Document Update	Ayala Eligoola Saridarov @ Ai-Law & Tech
4.0	January 1, 2025	Updates	
	14 Oct 2024	Approved	John Hanchak, CPO
	21 Oct 2024	Approved	Will Pospisil, CFO
	28 Oct 2024	Approved	Doug Shepard, President NA
	14/11/2024	Approved	Ronit Rubin, EMEA President
	21/11/2024	Approved	Joanne Pallas, President Global Operations
	26/11/2024	Approved	Eran Gil, CEO
	January 3, 2025	updates	Ronit Israeli
4.0	Aug 4, 2025	Reviewed	Amir Carmi, CISO

Table Of Contents

Document Properties	0
Change & Revision History	1
1. Purpose	3
2. Scope	3
3. Reference & Related Documents	3
4. Terms and abbreviations	3
5. Responsibility	3
6. The Policy	3

1. Purpose

- 1.1. This policy explains the Privacy rules and regulations AllCloud adheres to and the measures it takes to protect the privacy of the information it has access to.

2. Scope

- 2.1. 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.

3. Reference & Related Documents

- 3.1. ISO27001 Standard, Control 5.34

4. Terms and abbreviations

- 4.1. **Personal Data**- "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"
- 4.2. **CCPA**- California Consumer Privacy Act of 2018.
- 4.3. **GDPR**- General Data Protection Regulation (GDPR) (EU) 2016/679".
- 4.4. **CPRA**- California Privacy Rights Act (Civil Code Section 1798.100, et seq.)
- 4.5. **HIPPA** - Health Insurance Portability and Accountability Act of 1996.
- 4.6. **U.S. State Privacy Laws** – Refers to additional state-level privacy legislation in the United States that governs the rights of residents and obligations of businesses, alongside the CCPA and CPRA.

5. Responsibility

- 5.1. DPO is responsible for updating the Policy

6. The Policy

- 6.1. 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]
- 6.2. **Privacy Statement**

- 6.2.1. We, at AllCloud, Inc. and its subsidiaries (AllCloud BSD Ltd., AllCloud Platforms Ltd., AllCloud Business Applications Ltd., AllCloud Romania S.R.L., AllCloud

GmbH, AllCloud USA LLC, AllCloud ULC, and AllCloud Canada Inc.) (all together, hereinafter: "AllCloud" and/or "We"), respect your privacy and are firmly committed to keeping secure any information we obtain from you or about you.

- 6.2.2. As a global cloud solutions provider, the collection and use of personal data are essential to delivering our services, communications, and operations. We recognize the importance of safeguarding your information and complying with applicable privacy and data protection laws.
- 6.2.3. This Privacy Policy explains how we collect, use, share, and protect personal data in connection with your interactions with AllCloud, whether through our websites (<https://allcloud.io/>), services, communications, or events (collectively, the "Services").

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

6.3. SCOPE OF THIS PRIVACY POLICY

- 6.3.1. This Privacy Policy outlines our practices regarding the collection, use, and protection of:
 - 6.3.1.1. Personal Data – Information that identifies or relates to an individual and may include details such as name, identification number, location data, online identifiers, or factors specific to a person's physical, mental, economic, or social identity, as defined under all as defined by the General Data Protection Regulation ("GDPR") (EU) 2016/679. This may also include Protected Health Information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 and its attendant regulations ("HIPAA").
 - 6.3.1.2. California Consumer Information – Information related to individuals residing in California, as defined under the California Consumer Privacy Act of 2018 ("CCPA") and as amended by the California Privacy Rights Act ("CPRA") (Civil Code Section 1798.100, et seq.) (collectively "California Law"). This includes information that identifies, relates to, or could reasonably be linked to a California resident or household.
 - 6.3.1.3. 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 California Consumer information: (i) publicly available information or lawfully obtained, truthful Information that is a matter of public concern; (ii) de-identified or aggregated California Consumer information.

6.4. INFORMATION WE COLLECT

- 6.4.1. Depending on the context of your interaction with us, we may collect the following categories of personal data:

- 6.4.1.1. Identity and Contact Data: Full name, job title, employer, email address, telephone number, business address.
- 6.4.1.2. Account and Access Data: Login credentials, user identifiers, permissions, and roles.
- 6.4.1.3. Commercial and Transaction Data: Service usage details, billing information, contracts, purchase history.
- 6.4.1.4. Technical Data: IP address, device identifiers, system logs, browser type, network information.
- 6.4.1.5. Marketing and Communication Data: Preferences, survey responses, event participation, communication records.
- 6.4.1.6. Support and Service Operations Data: Data submitted in connection with support requests, system diagnostics, and managed services.
- 6.4.1.7. Recruitment Data (if you apply for a role): CV, employment history, education, and references.
- 6.4.1.8. California Consumers' Information Collection:

Category	Collected
A. Identifiers.	YES
B. Personal Information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	YES
C. Protected classification characteristics under California or federal law.	NO
D. Commercial information.	YES
E. Biometric information.	NO
F. Internet or other similar network activity.	YES
G. Geolocation data.	NO
H. Sensory data.	NO
I. Professional or employment-related information.	YES
J. Non-public education information (per the Family Educational Rights and Privacy Act).	NO
K. Inferences drawn from other Personal Information.	NO
L. Sensitive Personal Information	YES

- 6.4.1.9. We do not intentionally collect sensitive personal data unless explicitly required for a legitimate business purpose and subject to applicable legal safeguards.

6.5. HOW WE COLLECT PERSONAL DATA

- 6.5.1. We obtain personal information from the following sources:
 - 6.5.1.1. Information You Provide Directly: Your name, email, phone number, job title, company, payment information, or any other information you

provide when registering for our services, contacting support, attending events, or interacting with us.

6.5.1.2. Automatically Collected Information: This includes IP address, device type, browser type, usage data, and other identifiers collected through cookies, analytics tools, and similar technologies when interacting with our website or services.

6.5.1.3. Information from Third Parties: We may receive information from our business partners, service providers, or publicly available sources.

6.6. HOW WE USE PERSONAL INFORMATION

6.6.1. We use your personal information for the following purposes:

6.6.1.1. To deliver, operate, and improve the AllCloud Services.

6.6.1.2. To provide customer support and respond to your inquiries.

6.6.1.3. To manage billing, payments, and account administration.

6.6.1.4. To personalize your experience and recommend relevant services.

6.6.1.5. To send administrative or promotional communications.

6.6.1.6. To comply with legal obligations or protect our rights and interests.

6.6.1.7. For any other purpose disclosed to you or with your consent.

6.7. LEGAL BASIS FOR THE PROCESSING OF PERSONAL DATA

6.7.1. Suppose you are located in the European Economic Area (EEA), the United Kingdom, or another jurisdiction that requires a legal basis for processing personal data. In that case, our legal basis for collecting and using the personal information described in this Privacy Notice will depend on the type of data and the specific context in which we collect it. We typically process personal data on the following legal bases:

6.7.1.1. Performance of a Contract: When the processing is necessary to fulfill our contractual obligations to you or to take steps at your request before entering into a contract.

6.7.1.2. Legitimate Interests: When the processing is necessary for our legitimate business interests, such as to operate and improve our services, communicate with you, or detect and prevent fraud, except where your rights and interests override such interests.

6.7.1.3. Compliance with Legal Obligations: When the processing is necessary for compliance with a legal obligation.

6.7.1.4. Consent: Where you have given us consent to do so for a specific purpose. You may withdraw your consent at any time.

6.8. HOW WE USE AND PROCESS YOUR DATA

- 6.8.1. We use your personal information in a manner consistent with this Privacy Notice and applicable laws and regulations. Uses include:
- 6.8.1.1. Processing and Analytics: To provide Services and operate our business, including analysing usage and performance.
 - 6.8.1.2. Specific Purpose: To fulfill the particular purpose for which the data was provided (e.g., responding to an inquiry).
 - 6.8.1.3. Internal Business: To improve the AllCloud Services and website, enforce policies, and manage our operations.
 - 6.8.1.4. Marketing: We may send you promotional communications, 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. You may opt out at any time by contacting dpo@allcloud.io.
 - 6.8.1.5. Statistics: To create anonymized and aggregated statistics.
 - 6.8.1.6. Security and Dispute Resolution: To protect the security of our Website and Services, to detect and prevent cyberattacks, fraud, phishing, identity theft, data leaks, to verify genuine software licenses, or to resolve disputes.
 - 6.8.1.7. Development and Customer Support: Our teams may access personal data for support or development purposes, subject to strict confidentiality obligations.
 - 6.8.1.8. Law Enforcement: To comply with legal obligations or respond to legitimate requests from authorities, 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.
 - 6.8.1.9. Other Purposes: You will be informed of any new use that is not covered in this Privacy Notice.
 - 6.8.1.10. Protected Health Information (PHI): We will only use or disclose PHI with your written authorization, which may be revoked at any time in writing. We will no longer use or disclose PHI if you revoke your permission. However, you understand that we cannot take back any disclosures we have already made with your permission and that we are required to retain our records of the Services we provided to you.
 - 6.8.1.11. Non-Personal Data: We may use non-identifiable data without restriction.

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.

6.9. TRANSFER, SHARE, DISCLOSE, AND SALE OF DATA

- 6.9.1. For the purposes of the CCPA and other applicable privacy laws, AllCloud does not “sell” or “share” Personal Data. However, we may use analytics tools, cookies, and similar technologies (as described in this Privacy Policy) to help us analyze usage and improve our Services. In some jurisdictions, such use may be interpreted as a “sale” or “sharing” of Personal Data. Where required by law, you may opt out of such use by contacting us at dpo@allcloud.io.
- 6.9.2. We may share it for the aforementioned purposes with:
- 6.9.2.1. **Affiliates:** We may disclose Personal Data to our affiliates, meaning an entity that controls, is controlled by, or is under common control with AllCloud. Our affiliates may use this Personal Data in a manner consistent with this Privacy Policy.
 - 6.9.2.2. **Vendors and Service Providers:** To assist us in meeting business operations needs and to perform certain services and functions, we may disclose Personal Data to vendors and service providers, including providers of hosting services, customer service vendors, cloud services, content delivery services, support and safety monitoring services, email communication software, web analytics services, payment and transaction processors, and other information technology providers. Under our instructions, these parties will access, process, or store Personal Data only in the course of performing their duties to us.
 - 6.9.2.3. **Government Authorities:** We may share your Personal Data, including information about your interaction with our Services, with government authorities, or other third parties in compliance with the law (i) if required to do so to comply with a legal obligation, or in the good faith belief that such action is necessary to comply with a legal obligation, (ii) to protect and defend our rights or property, (iii) if we determine, in our sole discretion, that there is a violation of our terms, policies, or the law; (iv) to detect or prevent fraud or other illegal activity; (v) to protect the safety, security, and integrity of our products, employees, users, or the public, or (vi) to protect against legal liability.
 - 6.9.2.4. **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 under the terms of this Privacy Policy.

- 6.9.3. To provide our Services, manage and operate our business, we use third-party cloud services such as:
 - 6.9.3.1. Amazon Cloud Services comply with the GDPR and are ISO 27001, 27017, and 27018 certified (for AWS's full statement, see [All AWS Services GDPR ready | AWS Security Blog](#)). AllCloud stores some of its Information, which may contain Personal Data, at AWS cloud services in the Ireland region (eu-west-1).
 - 6.9.3.2. Google Workspace services are committed to GDPR compliance. (For Google Cloud full statement see <https://cloud.google.com/security/gdpr/>).
 - 6.9.3.3. Salesforce cloud services will comply with the GDPR in the delivery of their services and are ISO 27001, 27017, and 27018 certified (for a Salesforce full statement, see <https://www.salesforce.com/eu/campaign/gdpr/>).

6.10. INTERNATIONAL DATA TRANSFERS

- 6.10.1. AllCloud, Inc. is based in the United States and maintains subsidiaries outside of the United States, including Canada, Israel, Germany, and Romania. Information about you may be transferred to and processed in countries that may be different from the country in which you reside. These other countries may have data protection laws that are different from the laws of your country and, in some cases, may not be as protective. We have adopted appropriate safeguards, including implementing high levels of information security techniques; technical measures and/or contractual obligations to require that your information will remain protected in accordance with this Privacy Policy.
- 6.10.2. We may transfer Personal data to the following countries: Israel, US, Canada, Romania, India, and Germany, where we maintain our facilities and/or provide our services. The EU considers Israel and Canada as having adequate data protection laws. AllCloud Germany and Romania facilities comply with the GDPR. In addition to the many security and privacy controls we have put in place, we also use the EU's Standard Contractual Clauses as a valid transfer mechanism according to the GDPR when we need to transfer Personal Data to the US region.

6.11. DATA RETENTION AND ARCHIVES

- 6.11.1. 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.
- 6.11.2. 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.

6.12. PERSONAL DATA SECURITY

- 6.12.1. We are strongly committed to protecting your personal data and information, and we take reasonable technical and organizational measures, accepted in our industry, to keep your information secure and protect it against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. However, no network, server, database, or transmission over the internet is fully secure or error-free. Please use caution when sharing information online.
- 6.12.2. If you become aware of any security vulnerability or suspect a data breach, please report it promptly to us at dpo@allcloud.io.
- 6.12.3. We recommend you use, disclose, and share your personal data cautiously and only when necessary. While we take appropriate steps to protect data in transit and at rest, we cannot guarantee absolute security over the internet or control how third parties may use information you choose to share.
- 6.12.4. AllCloud implements legal, technical, and organizational information security measures based on internationally recognized standards. We are certified under:
 - 6.12.4.1. ISO/IEC 27001:2022 – Information Security Management Systems;
 - 6.12.4.2. ISO/IEC 27017:2015 – Code of practice for information security controls for cloud services.
- 6.12.5. and implements legal, technical, and organizational information security measures based on the ISO certification mechanisms specified in ISO/IEC 27018:2019—Protection of personally identifiable information (PII) in public clouds, acting as PII processors.

6.13. YOUR RIGHTS

- 6.13.1. Depending on your jurisdiction, you may have certain rights regarding your Personal Data under applicable privacy laws, including the GDPR, the California Consumer Privacy Act (CCPA) and other applicable U.S. state privacy laws, as well as the Health Insurance Portability and Accountability Act (HIPAA). These rights include, but are not limited to, the following:
- 6.13.2. Right to Access and Data Portability. You may have the right to request access to the Personal Data we hold about you and to receive a copy of such data in a portable, structured, and commonly used format. This includes:
 - 6.13.2.1. The categories of Personal Data we have collected about you.
 - 6.13.2.2. The specific pieces of Personal Data we have collected.
 - 6.13.2.3. The categories of sources from which the Personal Data was collected.
 - 6.13.2.4. The business or commercial purposes for collecting or sharing your Personal Data.
 - 6.13.2.5. The categories of third parties with whom your Personal Data has been shared.

- 6.13.3. Right to Correction (Rectification). You have the right to request the correction of inaccurate or incomplete Personal Data that we maintain about you.
- 6.13.4. Right to Deletion (Erasure). You may request the deletion of your Personal Data, subject to certain exceptions. Once we verify your identity and request, we will delete your Personal Data from our records and instruct our service providers to do the same, unless an exception applies. For example, we may deny deletion requests if retention is necessary to:
 - 6.13.4.1. Complete a transaction or provide a service you requested.
 - 6.13.4.2. Detect and prevent security incidents or fraudulent activity.
 - 6.13.4.3. Debug to identify and repair errors.
 - 6.13.4.4. Comply with a legal obligation.
 - 6.13.4.5. Enable internal uses aligned with your expectations.
 - 6.13.4.6. Exercise or defend legal claims.
 - 6.13.4.7. Conduct scientific, historical, or statistical research under appropriate safeguards.
- 6.13.5. Right to Receive an Accounting of Disclosures (Applicable under HIPAA). Where applicable, you may have the right to receive an accounting of certain disclosures we have made of your Protected Health Information (PHI).
- 6.13.6. Right to Object. You may object to the processing of your Personal Data on grounds relating to your particular situation, especially where we rely on legitimate interests as a legal basis. To exercise this right, please contact us at dpo@allcloud.io.
- 6.13.7. Right to Restrict Processing. You may request that we restrict the processing of your Personal Data if:
 - 6.13.7.1. The accuracy of the Personal Data is contested.
 - 6.13.7.2. The processing is unlawful, and you oppose erasure.
 - 6.13.7.3. We no longer need the data, but you require it for the establishment, exercise, or defense of legal claims.
 - 6.13.7.4. You have objected to processing, pending the verification of whether our legitimate grounds override yours.
- 6.13.8. Right to Non-Discrimination. We will not discriminate against you for exercising any of your rights under applicable privacy laws. Unless permitted by law, we will not:
 - 6.13.8.1. Deny you access to our Services.
 - 6.13.8.2. Provide you a different level or quality of Services.

6.13.8.3. Charge you different prices or rates for the Services.

6.13.9. Exercising Your Rights. To exercise any of the rights described above, please contact us at: Email: dpo@allcloud.io. Only you, or an authorized representative (such as a person registered with the California Secretary of State), may submit a verifiable request related to your Personal Data. California residents may submit such requests up to twice within a 12-month period. Your request must: Provide sufficient information for us to reasonably verify you are the person (or an authorized representative) whose Personal Data we collected; and Describe your request in sufficient detail for us to understand, evaluate, and respond appropriately. We cannot respond to your request if we cannot verify your identity or authority. Any information provided in connection with a rights request will be used solely to verify the requestor's identity or authority.

6.13.10. Response Time and Format. We will respond to verifiable requests: Within 45 days under California law (CCPA/CPRA); Within 30 days under the GDPR. If additional time is required, we will inform you in writing and provide the reason for the extension. Our response will be delivered by email unless otherwise requested. For California residents, our response will cover only the 12-month period preceding the request. If we cannot comply with your request, we will explain the reasons in our response. We do not charge a fee to process your request unless it is manifestly unfounded, repetitive, or excessive. In such cases, we will notify you in advance and provide a cost estimate.

6.14. ACCESS TO THIRD PARTY SERVICES

6.14.1. 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.

6.15. COOKIES

6.15.1. We use cookies and similar tracking technologies (such as web beacons and scripts) to enhance your experience, analyze website usage, and improve our services. Cookies are small text files stored on your device that may include an anonymous unique identifier.

6.15.2. Cookies allow a website to recognize your device and remember information such as your preferences or past actions. Some cookies are deleted when you close your browser (session cookies), while others remain on your device for a set period (persistent cookies).

6.15.3. We use the following types of cookies: necessary — required to make the website usable by enabling basic functions; preference — enables the website to

remember information that changes the way the website behaves or looks, like your preferred language; statistics — helps website owners understand who visitors interact with the website by collecting data anonymously; and marketing — which is used to deliver personalized content or ads.

- 6.15.4. We rely on our legitimate interest to use strictly necessary cookies. All other cookies are used only with your explicit consent, in accordance with applicable data protection laws (such as the GDPR).

6.16. USE OF ARTIFICIAL INTELLIGENCE (AI)

- 6.16.1. We use artificial intelligence and machine learning technologies to improve and personalize the services we provide to you. AI helps us analyze usage data, optimize service delivery, and tailor interactions to better meet your needs. For example, AI may be used to automate routine tasks, enhance customer support, or offer customized recommendations based on your preferences.
- 6.16.2. All data processed through AI technologies is handled securely and in compliance with applicable data protection laws. As outlined in this Privacy Policy, you have rights related to your personal data and any automated decisions.

6.17. CHANGES TO THIS PRIVACY POLICY

- 6.17.1. The Services and our business may change from time to time. As a result, it may be necessary to make changes to this Privacy Policy. At our sole discretion, we reserve the right 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.
- 6.17.2. Please review this Privacy Policy periodically, especially before providing 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.

6.18. GENERAL INQUIRIES AND COMPLAINTS

- 6.18.1. If you have an inquiry about AllCloud’s privacy practices, write to us at: dpo@allcloud.io.
- 6.18.2. You may have the right to complain to a supervisory authority. However, before doing so, you are welcome to contact us by email at dpo@allcloud.io to resolve the issue for the benefit of all parties.
- 6.18.3. The Israeli, German, and Romanian Data Protection authorities are our supervisory authorities. Contact information for EU Supervisory Authorities is available here: https://edpb.europa.eu/about-edpb/board/members_en. If you

believe your rights regarding PHI have been violated, you can file a complaint with us using the contact details below or with the U.S. Department of Health and Human Services (HHS).