

ISMS- A.5.34- Privacy Policy

Document Properties

Internal ID:	20241106005
Revision:	4.0
Date of revision:	August 12, 2024
Created by:	Admit Ivgi, CISO, DPO
Approved by:	Admit Ivgi, CISO, DPO
Confidentiality Level:	Public
Pages:	16

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, CISO, DPO
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	August 12, 2024	Document Update with HIPAA relevance	Mor Meshulam Moldovan, adv. @ Ai-Law & Tech

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. The purpose of this policy is to share the Privacy rules and regulations AllCloud adheres to and the measures that 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
- 4.3. **GDPR**- General Data Protection Regulation.
- 4.4. **CPRA**- California Privacy Rights Act

5. Responsibility

- 5.1. DPO is responsible to update the Policy

6. The Policy

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.

6.1. 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 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.

6.1.1. This Privacy Policy sets forth our policy with respect to:

6.1.1.1. 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**”). Personal Data may include Protected Health Information (“**PHI**”) as defined by the Health Insurance Portability and Accountability Act of 1996 and its attendant regulations (“**HIPAA**”).

6.1.1.2. As it refers to California’s consumers or individuals where their data is collected in the state of California (“**California Consumer**”), this Privacy Policy sets forth as a notice for our policy with respect to Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with you or your household, all as defined by 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**”).

6.1.1.3. “**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 (“Publicly available” means: Information that is lawfully made available from federal, state, or local government records or such information that a business has a reasonable basis to believe is lawfully made available to the general public by the California Consumers or from widely distributed media, or by the California Consumer; or information made available by a person to whom the California Consumer has disclosed the information if the California Consumer has not restricted the Information to a specific audience); (ii) de-identified or aggregated California Consumer information;

6.1.2. 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.

6.2. DATA WE COLLECT OR RECEIVE.

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

- 6.2.1.1. AllCloud uses, receives, collects, processes or stores only that Information which is necessary to provide its services and operate its business.
- 6.2.1.2. AllCloud doesn't collect and/or store customer's end data (Personal data about the customer's client/data that is stored in its system/environments) , though granted access by the Customer to its environments in order to provide the services. AllCloud secures the access and processes the data according to this policy as may be applicable to the provided services.
- 6.2.1.3. 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:
 - 6.2.1.3.1. Name, phone, email address, personal/physical address;
 - 6.2.1.3.2. Representative personal contact details, phone and cellphone numbers financial information (i.e. billing information, bank account information, credit card information), VAT Number, signature,
 - 6.2.1.3.3. 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;
 - 6.2.1.3.4. 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.
- 6.2.1.4. Cookies. We use cookies and similar tracking technologies (i.e. Google analytics) 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 are 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:
 - 6.2.1.4.1. Session cookies – for operating our Websites.
 - 6.2.1.4.2. Preference cookies – for remembering your preferences and various settings.

6.2.1.4.3. Security cookies – for security purposes.

6.2.2. California Consumers information collection. We have collected the following categories of Personal Information as defined under California Laws from California Consumers within the last twelve (12) months and as indicated here above:

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

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

- 6.2.3.1. **Directly from you.** For example, through information we ask from you when our clients or their agents engage our Services.
- 6.2.3.2. **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.
- 6.2.3.3. **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.
- 6.2.3.4. **From Third Parties that contract with us or interact with us in connection with the services we provide.** For example, from (i) vendors and partners that help us to build contact lists, supplement or update your information in our database, or confirm/verify our records and information are accurate and up to date, (ii) third parties that may contact you, on our behalf, to provide you relevant content and/or to become a member, or (iii) third parties (including,

other B2B contact providers) that integrate their services with ours or provide us access to their services.

- 6.2.4. Legal Basis for the Processing of Personal Data. 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.

6.3. USE AND PROCESS OF DATA.

- 6.3.1. 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 for business and commercial purposes as follows:
- 6.3.2. **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.
- 6.3.3. **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.
- 6.3.3.1. **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.).
- 6.3.3.2. **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.
- 6.3.3.3. **Statistics:** We may use any Personal Data you provide us with to generate statistical reports containing aggregated information.
- 6.3.3.4. **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.

- 6.3.3.5. **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.
- 6.3.3.6. **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.
- 6.3.3.7. **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.
- 6.3.4. **Other Uses Of PHI:** Other uses and disclosures of PHI not covered by this policy will be made only with your written permission. If you provide us permission to use or disclose PHI, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose PHI about you for the reasons covered by your written authorization. You understand that We are unable to take back any disclosures We have already made with your permission and that We are required to retain our records of the Services that We provided to you.
- 6.3.5. 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.
- 6.3.6. **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.

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

- 6.4.1. We do not sell Personal Data to third parties.
- 6.4.2. We may disclose your Personal Data with third parties for the mentioned-above business and commercial purposes. In the past 12 months, we have disclosed your Personal Information with the following categories of third parties:
 - 6.4.2.1. Partner, contractors and service providers. 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 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-mentioned categories of Personal Data.

- 6.4.2.2. 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.
- 6.4.2.3. 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.
- 6.4.3. In order to provide our Services, manage and operate our business, we use third parties cloud services such as:
 - 6.4.3.1. 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).
 - 6.4.3.2. Google Workspace services which are committed to GDPR compliance. (For Google Cloud full statement see <https://cloud.google.com/security/gdpr/>).
 - 6.4.3.3. Salesforce cloud services which will comply with the GDPR in the delivery of their services and is ISO 27001, 27017,27018 certified (for a Salesforce full statement see <https://www.salesforce.com/eu/campaign/gdpr/>).
- 6.4.4. 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 and HIPAA.

6.5. INTERNATIONAL DATA TRANSFERS.

- 6.5.1. 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.

- 6.5.2. 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. Israel and Canada are considered by the EU as having adequate data protection laws. AllCloud Germany and Romania facilities comply with the GDPR.
- 6.5.3. In addition to the many security and privacy controls that 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.

6.6. DATA RETENTION AND ARCHIVES

- 6.6.1. 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.
- 6.6.2. 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.

6.7. PERSONAL DATA SECURITY

- 6.7.1. 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.
- 6.7.2. 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.
- 6.7.3. 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.
- 6.7.4. AllCloud implements legal, technical and organizational information security measures based on the ISO certification mechanisms specified in ISO 27001:2022 – 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.

6.8. YOUR RIGHTS.

6.8.1. Right to Access and Data Portability.

- 6.8.1.1. You may have the right to request access to some of your Personal Data being stored by us.
- 6.8.1.2. You may have the right to request a physical or electronic copy of your PHI from our records.
- 6.8.1.3. California Consumers 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.
- 6.8.1.4. Once we receive and confirm your verifiable consumer or individual request, we will disclose to you, inter alia:
 - 6.8.1.4.1. The categories of personal information we collected about you.
 - 6.8.1.4.2. Our business or commercial purpose for the collecting of that personal information.
 - 6.8.1.4.3. The categories of third parties with whom we share that personal information.
 - 6.8.1.4.4. The specific pieces of personal information we collected about you (also called a data portability request)

6.8.2. Right to Correct.

- 6.8.2.1. You have the right to request that we correct inaccurate Personal Data that we maintain, or which pertains to you.

6.8.3. Right to Deletion.

- 6.8.3.1. You can also 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.
- 6.8.3.2. According to the California Law, we may deny California consumer's deletion request if retaining the information is necessary for us or our service providers to:
- 6.8.3.3. 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.
- 6.8.3.4. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- 6.8.3.5. Debug products to identify and repair errors that impair existing intended functionality.

- 6.8.3.6. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
- 6.8.3.7. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 seq.).
- 6.8.3.8. 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 deletion may likely render impossible or seriously impair the research achievement if you previously provided informed consent.
- 6.8.3.9. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
- 6.8.3.10. Comply with a legal obligation.
- 6.8.3.11. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.
- 6.8.4. Right to Receive an Accounting of Disclosures. You may have the right to receive a list of disclosures We made of your PHI.
- 6.8.5. Right to Object.
 - 6.8.5.1. If you wish to object to processing, you are required to contact us at dpo@allcloud.io.
- 6.8.6. Right to Restrict Processing.

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

 - 6.8.6.1. The Personal Data is PHI;
 - 6.8.6.2. The accuracy of the Personal Data is contested by the data owner;
 - 6.8.6.3. The processing is unlawful, and the data owner objects to having their Personal Data erased, instead requesting that its use be restricted;
 - 6.8.6.4. 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;
 - 6.8.6.5. The data owner has objected to processing pending verification of whether the legitimate grounds of your service provider override those of the data owner.
- 6.8.7. Right to Non-Discrimination.
 - 6.8.7.1. We will not discriminate against you for exercising any of your California Law, HIPAA, or GDPR rights. Unless permitted by the California Law, HIPAA and GDPR, we will not: Deny your use of our Services and/or Provide you a different level or quality of Services.
- 6.8.8. Exercising your Rights.

- 6.8.8.1. In order to exercise these rights, you can contact us at: Email: dpo@allcloud.io; or call us at: 1-800 416-8949 (Toll free number).
- 6.8.8.2. 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.
- 6.8.8.3. The verifiable consumer or individual request must:
 - 6.8.8.3.1. Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
 - 6.8.8.3.2. Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.
- 6.8.8.4. **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.
- 6.8.9. Response Timing and Format.
 - 6.8.9.1. We endeavor to respond to a verifiable consumer request within 45 days (by the California Law) 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.
 - 6.8.9.2. 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.

6.9. ACCESS TO THIRD PARTY SERVICES.

- 6.9.1. This Privacy Policy does not apply to any Personal Data that you provide to third parties.
- 6.9.2. 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.

6.10. CHANGES TO THIS PRIVACY POLICY

- 6.10.1. 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. 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.
- 6.10.2. 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.

6.11. DISPUTE RESOLUTION

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

6.12. GENERAL INQUIRIES AND COMPLAINTS.

- 6.12.1. 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.
- 6.12.2. 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. If you believe your rights regarding PHI have been violated, complaints can be filed with us, using the contact details below, or with the U.S. Department of Health and Human Services (HHS).

6.13. CONTACT DETAILS

- 6.13.1. We will take reasonable steps to work with you to attempt to resolve your complaint. You may contact us at:

7.

Location	ISRAEL and (HEADQUARTERS)	GERMANY (MUNICH)	ROMANIA	USA- California
Contact Person	Admit Ivgi, DPO	Admit Ivgi, DPO	Admit Ivgi, DPO	Admit Ivgi, DPO
Address	13 Amal St., Building A, 2nd Floor. POB: 11390 Rosh Haayin, 4809280	Rechtsanwaltsgesells chaft mbH Prinzregentenstr. 78 Munich, 81675 Germany	Strada George Enescu 23 București, 010303 Romania	
Contact info	Tel: +972 (3) 6783868 Fax: +972 (3) 5048647 Email: dpo@allcloud.io	Email: dpo@allcloud.io	Email: dpo@allcloud.io	Email: dpo@allcloud.io Tel: 1-800 416-8949 (Toll free number)