Cassiopeia

Cassiopeia's Remote Work Solution - Privacy Policy

At Cassiopeia, we take your privacy seriously. We are committed to maintaining the confidentiality and security in regard to our users' personal information. We collect only the information necessary for providing Cassiopeia's product and Services.

We understand that you care about how your information is used and shared. This Privacy Policy explains the types of information that is collected by Cassiopeia and stored on its servers, as well as how this information is used. We will not use or share your information with anyone except as described in this Privacy Policy.

When you use Cassiopeia, you give your consent to the collection, use, and disclosure of your information as described in this Privacy Policy. If you disagree with any term provided herein, you may not use the site and/or Service.

In this Privacy Policy, a reference to:

- **Customer** means the person or entity that has contracted with Cassiopeia to allow to use Cassiopeia's Services;
- **Employee** means any person who works at the Customer's company;
- **Service** means all products, services, and Websites offered by Cassiopeia;
- **Visitor** means any person who visits our Websites;
- **You** or **your** means either an Employee or Customer, as applicable;
- **Website** means www.cassiopeia.tech.

The information we collect

Information we generally collect

- Usage information: We obtain non-personal information through your use of Cassiopeia. Non-personal information is any unconcealed information that is available to us while users use our Service. We are not aware of the identity of the user from which we have collected such non-personal information. This information consists of technical and behavioral information, such as, but not limited to, the user's click-stream on the site, the length of a user's visit on the Site, etc.
  We collect non-personal information for research purposes and in order to learn how our users use Cassiopeia so we can improve our product accordingly.

Information we collect from Employees and Customers

- Contact information: When you provide us with your contact information, whether through the use of our Services or interaction with Cassiopeia's Employees, we collect your contact information. This information may include your name and email address.

- Demographic and workplace-related data: Customers may provide us with additional demographic information such as the role, age, gender, and tenure of their Employees.
- HRIS data: If the Customer uses a third-party Human Resource Information System to import information into the Services, we will also receive information from that third-party (for example, the Employee's company email address, name, Employee unique ID, employment data).
- Survey data: When you answer a Customer survey, we may store your survey answers and comments.
- Communication Metadata: We obtain this information via APIs or directly from the Customer. This information can include metadata from email, video platforms, the workplace chat platform, or any other communication platform metadata such as, but not limited to, thread ID, timestamps, sender's email address, and receiver's email address.

Please consider that you are not obligated by law to provide us with any personal information. You hereby acknowledge, warrant and agree that any information you do provide us is provided at your own free will and consent, for the purposes mentioned in this Privacy Policy, and that we may keep such personal information in databases which will be registered and kept in accordance with applicable laws.

The data controller and processor

Data protection law in certain jurisdictions differentiates between the "Data Controller" and "Data Processor". For Employees and Customers, the Customer will be considered as the controller of your personal information, and Cassiopeia will be the processor. For Visitors, Cassiopeia will be considered as the controller of your personal information.

Information collection process

There are two main methods we use:

1. We collect information through your use of Cassiopeia's Services. When you visit or use our Services, we are aware of it and may gather and collect information, either independently or with the help of third-party Services as detailed below.
2. We collect contact information that you voluntarily provide us with (for example, your name or email address), through the use of our services, a form on our website, or an interaction with our sales or customer support team.

The purposes for collecting information

We collect non-personal and personal information for the following purposes:

1. To provide and operate Cassiopeia's Services. For example, to monitor, maintain, and improve our Services.

2. To further develop, customize, and improve our Services and AI model, based on users' non-personal data.
3. To create de-identified aggregate data. To provide Customers with a better understanding of the results presented at Cassiopeia's dashboard, we use the information in a de-identified aggregate form to compare Customers' results to the results of other Customers or types of Customers. We also use your data to continually improve our Services, including our de-identified aggregate data sets. None of your survey data will be disclosed to other unrelated Customers in a non-aggregated or identifiable form.
4. To provide our users with ongoing Customer assistance and technical support.
5. To comply with applicable laws and regulations.
6. To be able to contact our users with general or personalized Service-related notices.
7. To make scientific advancements for research purposes.

Access to your personal information and third-party Services

We may use third-party Services and/or Services, for email or content delivering and/or saving and analyzing any non-personal data. Please note that the servers of third-parties' Service providers may be located outside of the European Union. Additionally, these third-party Services may receive or otherwise have access to our users' personal information and/or non-personal information.

Such Service providers include:

Service	Privacy policy is available at:
Google analytics	http://www.google.com/intl/en/analytics/privacyoverview.html
Cloudmailin	http://www.cloudmailin.com/privacy
Gmail	https://www.google.com/policies/privacy/
Survey monkey	https://www.surveymonkey.com/mp/legal/privacy-policy
Sendgrid	https://sendgrid.com/policies/privacy/
Twilio	https://www.twilio.com/legal/privacy
AWS	https://aws.amazon.com/privacy/
Google LLC	https://policies.google.com/privacy?hl=en-US
Cloudflare, Inc.	https://www.cloudflare.com/privacypolicy/
Wix	https://www.wix.com/about/privacy

In most cases, the information that we disclose to our staff or Service providers will be directly necessary in providing our Services to you. However, there may be occasions where we need to disclose your personal information to other third-parties or for other purposes, including:

- To prevent illegality or enforce our terms and policies;
- To protect our rights or the rights of our staff;
- To keep other entities associated with us informed;
- Pursuant to a legal request, such as a subpoena, legal proceedings, search warrant or court order, or in compliance with applicable laws, if we have a good faith belief that the law requires us to do so, with or without notifying you;
- To respond to the user's support requests/tickets;
- To respond to claims that contact details of a third-party have been inputted or transmitted without consent or as a form of harassment;
- To protect the rights, property, or personal safety of Cassiopeia or its users;
- If Cassiopeia undergoes any change in control, including by means of merger, acquisition, or purchase of substantially all of its assets;
- To collect, hold and/or manage personal information through Cassiopeia's authorized affiliates and third-party Service provider.
- To improve the system and make scientific advancements for research purposes.
- To share aggregated de-identified data for any purpose. For example, we may share aggregated de-identified data with Customers for business or research purposes.
- To disclose your personal information to our staff, suppliers, or professional advisors. These disclosures may be related to activities such as filling orders, processing payments, managing documents, research, or providing advice or consultation.

Retention

How long we retain your Personal Data depends on the type of data and the purpose for which we process the data. We will retain your Personal Information for the period necessary to fulfill the purposes outlined in this Privacy Policy unless a longer retention period is required or permitted by law.

For more information about Cassiopeai's retention period, please see the 'For how long do you retain my information?' section below.

If you wish to access, copy, correct or delete your personal information, please send us a request and we will provide you with information about whether we hold, or process on behalf of a third-party, any of your personal information. To request this information, please contact us at contact@cassiopeia.tech. Also, if you want to review, correct (if necessary), or delete the information that we have collected and held about you, please contact us at contact@cassiopeia.tech.
We will respond to requests to access as timely as possible.

Requests from Employees

If you are an Employee, we collect, hold, and process information about you on behalf, and under the direction, of the Customer. This information includes data uploaded to our Services by the Customer (for example, your name, email address and demographic data) and your survey responses and comments submitted through our Services.

Because we collect, hold and process your personal information on behalf of the Customer, you will need to contact the Customer if you want to correct, access, amend or delete any information we store about you.

You may contact the Customer directly, or Cassiopeia at contact@cassiopeia.tech. The request needs to be sent from the email address that was used within Cassiopeia's Service. Please note that by sending us a request, we may need to identify you and/or your survey responses to the Customer. We will respond to your request within a reasonable timeframe.

Users must keep the appropriate backup of their data. Cassiopeia shall not be responsible for any deletion of data, for any breach of its database, or for any erroneous data.

Note that although your aforementioned personal information may be removed from our databases, Cassiopeia will retain the non-personal information contained in the data you provided, and such information will continue to be used by us for the purpose of research, business, and product improvement.

For how long do you retain my information?

Visitors

We will retain your personal information for as long as it is necessary to provide our Services to you or to comply with our legal obligations, resolve disputes, and enforce our legal rights.

Employees

Employees' personal information such as communication data and survey responses will be deleted after 90 days from the date of data collection. After 90 days, the data insights gained from Customers and Employees are being anonymized and therefore do not constitute personal data.

The Employees' contact information, demographics, and workplace-related data, such as name, email address, and phone number, will be kept in our Service for as long as the Customer uses Cassiopeia's Services, in order to allow us to continue operating the Service.

Security and storage of information

We take your privacy and data security very seriously and strive to maintain the security of all personal information. Cassiopeia maintains appropriate physical, technical, and administrative safeguards to protect against the loss, misuse, or unauthorized access, use, disclosure, modification, or destruction of personal information and hosted data.
The personal information is hosted, maintained, and processed on Amazon Web Services' servers that are located within the United States. We may transfer, disclose, or process personal information to third parties (subject to 'Access to your personal information and third-party Services' section), which may be situated in another country. By using Cassiopeia, you agree to this storing, processing, and/or transfer of data.

We also gain data insights from Customers' and Employees' information that are used to improve Cassiopeia's model. Such data is anonymized and therefore does not constitute personal data.

Regardless of the measures and efforts taken by Cassiopeia, we cannot and do not guarantee the absolute protection and security of Employees', Visitors', and Customers' personal and non-personal information.
In the event that any personal information processed by Cassiopeia on behalf of a Customer is lost, stolen, or has been unauthorizedly accessed, we will notify the relevant Customer immediately and take remedial measures.

How do we use the information we collect?

We use your personal information for a variety of purposes. The information we collect and hold is reasonably necessary for our business, including providing you with our Services.
When you use our Services as a Customer or Employee, we process your personal information either:

- With your consent;
- To fulfill our contractual responsibility to deliver the Services to the Customer;
- To pursue Cassiopeia's legitimate interests in improving our Services or developing new products and features; or
- Based on the lawful basis of the processing is necessary for the purposes of carrying out the obligations and exercising specific rights in the field of employment and social security and social protection law.

When you use our Services as a Visitor, we process your personal information either:

- With your consent; or
- To pursue Cassiopeia's legitimate interests in improving our Services or developing new products and features.

Changes to our Privacy Policy

We may update this privacy policy to reflect changes to our policies and/or methods of

collecting, using, and storing information. Therefore, please review our privacy policy frequently. We will notify our users regarding substantial changes in this policy on Cassiopeia's homepage and/or by sending an email regarding such changes.

Contact us

If you have any questions or complaints about our compliance with this Privacy Policy or relevant privacy laws, please contact us at:

CASSIOPEIA SOCIAL INNOVATION LTD.
Shimon Ben Zvi 43 Givatayim,
Israel
Email: contact@cassiopeia.tech

Last Revised: 28/05/2020

Cassiopeia

Cassiopeia's Communication Channel - Privacy Policy

At Cassiopeia, we take your privacy seriously. We are committed to maintain the confidentiality and security in regards to our users' personal information. We collect only the information necessary for providing Cassiopeia's product and Services.

We know that you care about how your information is used and shared. This Privacy Policy explains the types of information that is collected by Cassiopeia and stored on its servers, as well as how this information is used. We will not use or share your information with anyone except as described in this Privacy Policy.

When you use Cassiopeia, you give your consent to the collection, use and disclosure of your information as described in this Privacy Policy. If you disagree with any term provided herein, you may not use the site and/or Service.

In this Privacy Policy, a reference to:

- **Administrator** means any person who has log-in credentials to a Customer account to manage that account or review Cassiopeia's dashboard;
- **Customer** means the person or entity that has contracted with Cassiopeia to allow to use Cassiopeia's Services;
- **Employee** means any person who work at the Customer's company;
- **Service** means all products, Services and Websites offered by Cassiopeia;
- **Visitor** means any person who visits our Websites;
- **You** or **your** means either an Administrator, Employee or Customer, as applicable;
- **Website** means www.cassiopeia.tech.

The information we collect

Information we generally collect

- Usage information: We obtain non-personal Information through your use of Cassiopeia. Non-personal information is any unconcealed information which is available to us while users use our Service. We are not aware of the identity of the user from which we have collected such non-personal information. This information consists of technical and behavioral information, such as, but not limited to, the user's click-stream on the site, the length of a user's visit on the Site, etc.
  We collect non-personal information for research purposes and in order to learn how our users use Cassiopeia so we can improve our product accordingly.

Information we collect from Employees

- Contact information: When you provide us with your contact information, whether through use of our Services or an interaction with Cassiopeia's Employees, we

collect your contact information. This information may include your name and email address.

- Demographic data: Customers may provide us with additional demographic information such as role, age, Gender Region, Tenure.
- HRIS data: If the Customer uses a third party human resource information system to import information into Services, we will also receive information from that third party (for example Employee's company email address, name, Employee unique id, employment data).
- Survey data: When you answer a Customer survey, we will store your survey answers and comments.
- Correspondence Metadata: Customers may provide us email metadata such as timestamps, sender's email address and receiver's email address.
- Private Employee email address - if you would like to consult anonymously via Cassiopeia communication channel, you will need to provide your email address. We require your email address so that the system may forward you any response(s) from the HR in your organization. If you choose to remain anonymous, your email address is kept secure and is not shown to the recipient. Please note that Cassiopeia does not store on its servers any part of your consultation content or of the HR representative response.

Information we collect from Administrators

- Administrator details: in order to allow employees to consult with the HR representative and feel comfortable while doing so, we will require the following information from the representative when setting up the Service: name, email address and picture. The representative's identifiers are transferred to Cassiopeia's Gmail account and may be stored on Google's servers (for more information regarding our use of third party Services, please review the 'Access to your personal information and third party Services' section). Cassiopeia will use the representative's identifiers only for providing Cassiopeia's Service within the organization at which the representative is employed.
- Cassiopeia's unique identifier: Cassiopeia sends the user's question, protected by password, to the representative in the organization, by using a unique identifier stored in Cassiopeia servers, that links together only the necessary information regarding a correspondence between the user and the officer. We link the following data to the unique identifier in order to link between the email addresses and the correspondence: the email address from which the question was sent, the email address to which the question was sent and the time of the correspondence.
- Survey data: When you create and launch surveys using our services, we will store those survey questions and other information related to those surveys.
- Session and local storage of the Administrator.

Please consider that you are not obligated by law to provide us with any personal information. You hereby acknowledge, warrant and agree that any information you do provide us is provided at your own free will and consent, for the purposes mentioned in this Privacy Policy, and that we may keep such personal information in databases which will be registered and kept in accordance with applicable laws.

The data controller and processor

Data protection law in certain jurisdictions differentiates between the "Data Controller" and "Data Processor". For Employees and administrators, the Customer will be considered as the controller of your personal information and Cassiopeia will be the processor. For Visitors, Cassiopeia will be considered as the controller of your personal information.

Information collection process There are two main methods we use:

1. We collect information through your use of Cassiopeia's Services. When you visit or use our Services, we are aware of it and may gather and collect information, either independently or with the help of third-party Services as detailed below.
2. We collect information which you provide us voluntarily. For example, we collect the email address you provided us when you choose to send a consultation to the HR representative in your organization, when sending us the HR representative's identifiers, employee metadata and/or when you contact us directly.

The purposes for collecting information

We collect non-personal and personal information for the following purposes:

1. To provide and operate Cassiopeia's Services. For example to monitor, maintain and improve our Services.
2. To further develop, customize and improve our Services and AI model, based on users' non-personal data.
3. Create de-identified aggregate data: To provide Customers with a better understanding of the results presented at Cassiopeia's dashboard, we use the information in a de-identified aggregate form to compare Customers' results to the results of other Customers or types of Customers. We also use your data to continually improve our Services, including our de-identified aggregate data sets. None of your survey data will be disclosed to other unrelated Customers in a non-aggregated or identifiable form.
4. To provide our users with ongoing Customer assistance and technical support.
5. To comply with applicable laws and regulations.
6. To be able to contact our users with general or personalized Service-related notices.

Access to your personal information and third party Services

We may use third party Services and/or Services, for email or content delivering and/or saving and analyzing any non-personal data. Please note that the servers of third parties' Services providers may be located outside of the European Union. Additionally, these third-party Services may receive or otherwise have access to our users' personal information and and/or non-personal Information.

Such Services include:

Service	Privacy policy is available at:
Google analytics	http://www.google.com/intl/en/analytics/privacyoverview.html
Mailgun	https://www.mailgun.com/privacy-policy
Cloudmailin	http://www.cloudmailin.com/privacy
Gmail	https://www.google.com/policies/privacy/
Survey monkey	https://www.surveymonkey.com/mp/legal/privacy-policy
Sendgrid	https://sendgrid.com/policies/privacy/
Vidgrid	https://www.vidgrid.com/privacy/
Twilio	https://www.twilio.com/legal/privacy
Google LLC	https://policies.google.com/privacy?hl=en-US
Cloudflare, Inc.	https://www.cloudflare.com/privacypolicy/
Wix	https://www.wix.com/about/privacy

In most cases, the information that we disclose to our staff or Service providers will be directly necessary to provide our Services to you. However, there may be occasions where we need to disclose your personal information to other third parties or for other purposes, including to:

- Prevent illegality or enforce our terms and policies;
- Protect our rights or the rights of our staff;
- Keep other entities associated with us informed;
- Pursuant to a legal request, such as a subpoena, legal proceedings, search warrant or court order, or in compliance with applicable laws, if we have a good faith belief that the law requires us to do so, with or without notifying you;
- To respond to user's support requests/tickets;
- To respond to claims that contact details of a third-party have been inputted or transmitted without consent or as a form of harassment;
- To protect the rights, property or personal safety of Cassiopeia or its users;
- If Cassiopeia undergoes any change in control, including by means of merger, acquisition or purchase of substantially all of its assets;

- To collect, hold and/or manage personal information through Cassiopeia's authorized affiliates and third-party Service provider.
- To share aggregated de-identified data for any purpose. For example, we may share aggregated de-identified data with Customers for business or research purposes.
- To disclose your personal information to our staff, suppliers or professional advisors. These disclosures may be related to activities such as filling orders, processing payments, managing documents, research, or providing advice or consultation.

Retention

How long we retain your Personal Data depends on the type of data and the purpose for which we process the data. We will retain your Personal Information for the period necessary to fulfill the purposes outlined in this Privacy Policy unless a longer retention period is required or permitted by law.

For more information about Cassiopeai's retention period, please see the 'For how long do you retain my information?' section below.

If you wish to access, copy, correct or delete your personal information, please send us a request and we will provide you with information about whether we hold, or process on behalf of a third-party, any of your personal information. To request this information, please contact us at contact@cassiopeia.tech. Also, if you want to review, correct (if necessary), or delete the information that we have collected and held about you, please contact us at contact@cassiopeia.tech.
We will respond to requests to access as timely as possible.

Requests from Administrators and Employee

If you are an Administrator or an Employee, we collect, hold and process information about you on behalf, and under the direction, of the Customer. This information includes data uploaded to our Services by the Customer (for example, your name, email address and demographic data) and your survey responses and comments submitted through our Services.

Because we collect, hold and process your personal information on behalf of the Customer, you will need to contact the Customer if you want to:

- Correct, access, amend or delete any information we store about you; or
- Stop receiving Customer's messages that are being sent using our Services.

You may contact the Customer directly, or Cassiopeia at contact@cassiopeia.tech. The request needs to be sent from the email address that was used within Cassiopeia's Service. Please note that by sending us a request, we may need to identify you and/or your survey responses to the Customer. We will respond to your request within a reasonable timeframe.

Users must keep the appropriate backup of their data. Cassiopeia shall not be responsible for any deletion of data or for any breach of its database or for any erroneous data.

Note that although your aforementioned personal information may be removed from our databases, Cassiopeia will retain the non-personal information contained in the data you provided, and such information will continue to be used by us for the purpose of research, business and product improvement.

How long do you retain my information?

Visitors

We will retain your personal information for as long as it necessary to provide our Services to you, or to comply with our legal obligations, resolve disputes, and enforce our legal rights.

Administrator

We retain your personal information for as long as we provide our Services to the Customer, or as needed to comply with our legal obligations, resolve disputes or enforce our legal rights.

Employees

We keep the user's personal email address for 3 months after user's last use of Cassiopeia communication channel. A user's last use will be considered as the last time the user corresponded with the HR representative via Cassiopeia.
Employees personal information such as demographic data and survey responses will be deleted after 90 days from the date of data collection. After 90 days the data insights gained from Customers and Employees are being anonymized, and therefore does not constitute as personal data.

The employees contact information such as name, email address and phone, will be kept in our Service for as long as the organization that person is employed at uses Cassiopeia's Services, in order to allow us to keep operating the Service.

Security and storage of information

We take your privacy and data security very seriously and strive to maintain the security of all personal information. Cassiopeia maintains appropriate physical, technical and administrative safeguards to protect against loss, misuse or unauthorized access, use, disclosure, modification, or destruction of personal information and hosted data.

The personal information is hosted ,maintained and processed on Amazon Web Services' servers that are located within the United States. We may transfer, disclosed or processed personal information to third parties (subject to 'Access to your personal information and

third party Services' section), which may be situated in another country. By using Cassiopeia, you agree to this storing, processing and/or transfer of data.

We do not store the content of anonymous consultations, the responses of the HR representative.We also gain data insights from Customers' and Employees' information that are used to improve Cassiopeia's model. Such data is anonymized, and therefore does not constitute as personal data.

Regardless of the measures and efforts taken by Cassiopeia, we cannot and do not guarantee the absolute protection and security of Employees and Administrators personal and non-personal information.

In the event that any personal information processed by Cassiopeia on behalf of a Customer is lost, stolen, or has been unauthorizedly accessed, we will notify the relevant Customer immediately and take remedial measures.

How do we use the information we collect?

We use your personal information for a variety of purposes. The information we collect and hold is reasonably necessary for our business, including providing you with our Services.

When you use our Services as an Administrator or Employee, we process your personal information either:

- With your consent;
- To fulfill our contractual responsibility to deliver the Services to the Customer; or
- To pursue Cassiopeia's legitimate interests of improving our Services or developing new products and features.
- Based on the lawful basis of processing is necessary for the purposes of carrying out the obligations and exercising specific rights in the field of employment and social security and social protection law.

When you use our Services as a Visitor, we process your personal information either:

- With your consent; or
- To pursue Cassiopeia's legitimate interests of improving our Services or developing new products and features.

Changes to our Privacy Policy

We may update this privacy policy to reflect changes to our policies and/or methods of collecting, using and storing information. Therefore, please review our privacy policy frequently. We will notify our users regarding substantial changes in this policy on Cassiopeia's homepage and/or send an email regarding such changes.

Contacting us

Cassiopeia

If you have any questions or complaints about our compliance with this Privacy Policy or relevant privacy laws, please contact us at:

CASSIOPEIA SOCIAL INNOVATION LTD.

Shimon Ben Zvi 43 Givatayim,

Israel

Email: contact@cassiopeia.tech

Last Revised: 28/05/2020

Cassiopeia

DATA PROCESSING ADDENDUM

This Data Processing Agreement ("**DPA**") forms part of the the Terms and Conditions ("**Agreement**") entered by and between you, the Customer (as defined in the Agreement) (collectively, "you", "Customer"), and Cassiopeia Social Innovation Ltd (" **Cassiopeia**", "**us**", "**we**", "**our**") to reflect the parties' agreement with regard to the Processing of Personal Data by Cassiopeia solely on behalf of the Customer. Both parties shall be referred to as the "Parties" and each, a "Party".

Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.

1. DEFINITIONS

a) "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

b) "**Authorized Affiliate**" means any of Customer's Affiliate(s) which is explicitly permitted to use the Services pursuant to the Agreement between Customer and Cassiopeia, but has not signed its own agreement with Cassiopeia and is not a "Customer" as defined under the Agreement.

c) "**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. seq.

d) The terms, "**Controller**", "**Data Subject**", "**Member State**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR. The terms "**Business**", "**Business Purpose**", "**Consumer**" and "**Service Provider**" shall have the same meaning as in the CCPA. For the purpose of clarity, within this DPA "Controller" shall also mean "Business", and "Processor" shall also mean "Service Provider". In the same manner, Processor's Sub Processor shall also refer to the concept of Service Provider.

e) **"Data Protection Laws"** means all privacy and data protection laws and regulations, including such laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland, the United Kingdom, the United States of America and any other law applicable to the Processing of Personal Data under the Agreement.

f) "**Data Subject**" means the identified or identifiable person to whom the Personal Data relates.

g) "**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

h) "**Personal Data**" or "**Personal Information**" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable natural person or Consumer (as defined in the CCPA), which is processed by Cassiopeia solely on behalf of Customer, in the course of performing its obligations under the the Agreement between Customer and Processor.

i) "**Sub Processor**" means any third party that Processes Personal Data under the instruction or supervision of Cassiopeia.

j) "**Standard Contractual Clauses**" means the standard contractual clauses and related annexes and appendices which are hereby incorporated into and form part of this DPA in the form available as Schedule 2 of this DPA ("**SCC**"), or with respect to onward transfers by Processor to a Sub-processor pursuant to Section C of Annex A of the SCC, also the standard contractual clauses for the transfer of personal data to processors or sub-processors established in third countries, as adopted by the European Commission from time to time under Directive 95/46/EC or the GDPR, as applicable.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties**. The Parties acknowledge and agree that with regard to the Processing of Personal Data performed solely on behalf of Customer, (i) Customer is the Controller of Customer Data (as defined in the Agreement), (ii) Cassiopeia is the Processor of Customer Data; (iii) for the purposes of the CCPA (and to the extent applicable), Customer is the "Business" and Cassiopeia is the "Service Provider" (as such terms are defined in the CCPA), with respect to Processing of Personal Data described in this Section 2.1. The terms "Controller" and "Processor" below hereby signify Customer and Cassiopeia, respectively.

2.2 **Customer's Processing of Personal Data**. Customer, in its use of the Services, and Customer's instructions to the Processor, shall comply with Data Protection Laws. Customer shall establish and have any and all required legal bases in order to collect, Process and transfer to Processor the Personal Data, and to authorize the Processing by Processor, and for Processor's Processing activities on Customer's behalf, including the pursuit of 'business purposes' as under the CCPA.

2.3 **Processor's Processing of Personal Data**. When Processing solely on Customer's behalf under the Agreement, Processor shall Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and this DPA; (ii) Processing for Customer to be able to use the Services; (iii) Processing to comply with Customer's reasonable and documented instructions, where such requests are consistent with the terms of the Agreement, regarding the manner in which the Processing shall be performed; (iv) rendering Personal Data fully anonymous, non-identifiable and non-personal; (v) Processing as required under any applicable laws to which Processor is subject; in such a case, Processor shall inform Customer of the legal requirement before Processing,

unless that law prohibits such information on important grounds of public interest.

To the extent that Processor cannot comply with an instruction from Customer, Processor (i) shall inform Customer, providing relevant details of the problem, (ii) Processor may, without any kind of liability to Customer, temporarily cease all Processing of the affected Personal Data (other than securely storing such data), (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, Customer may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and (iv) Customer shall pay to Processor all the amounts owed to Processor or due before the date of termination. Customer will have no further claims against Processor (including, without limitation, requesting refunds for Services) pursuant to the termination of the Agreement and the DPA as described in this paragraph.

2.4 **Details of the Processing**. The subject-matter of Processing of Personal Data by Processor is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Annex 1 (Details of the Processing) to this DPA.

2.5 **CCPA Standard of Care; No Sale of Personal Information**. Cassiopeia acknowledges and confirms that it does not receive or process any Personal Information as consideration for any services or other items that Cassiopeia provides to Customer under the Agreement. Cassiopeia shall not have, derive, or exercise any rights or benefits regarding Personal Information Processed on Customer's behalf, and may use and disclose Personal Information solely for the purposes for which such Personal Information was provided to it, as stipulated in the Agreement and this DPA. Cassiopeia represents and warrants that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling (as such term is defined in the CCPA) any Personal Information Processed hereunder, without Customer's prior written consent, nor taking any action that would cause any transfer of Personal Information to or from Cassiopeia under the Agreement or this DPA to qualify as "selling" such Personal Information under the CCPA.

3. RIGHTS OF DATA SUBJECTS

Data Subject Requests. Processor shall, to the extent legally permitted, promptly notify Customer if Processor receives a request from a Data Subject or Consumer to exercise their rights (to the extent available to them under applicable law) of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, its right not to be subject to an automated individual decision making, to opt-out of the sale of Personal Information, or the right not to be discriminated against for exercising any CCPA Consumer rights ("**Data Subject Request**"). Taking into account the nature of the Processing, Processor shall assist Customer by appropriate technical and organizational measures, insofar as this is possible and reasonable, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. Processor may refer Data Subject Requests received, and the Data Subjects making them, directly to the Customer for its treatment of such requests.

4. CASSIOPEIA PERSONNEL

4.1 **Confidentiality**. Processor shall ensure that its personnel engaged in the Processing of Personal Data have committed themselves to confidentiality.

4.2 **Permitted Disclosures**. Without derogating from Section 2.3 above and Section 5 below, Processor may disclose and Process the Personal Data (a) to the extent required by a court of competent jurisdiction or other competent governmental or semi-governmental authority, or (b) otherwise as required by applicable Data Protection Laws (in such a case, Processor shall inform the Customer of the legal requirement before the disclosure, unless legally prohibited from doing so), or (c) on a "need-to-know" basis under an obligation of confidentiality to its legal counsel(s), data protection advisor(s) and accountant(s).

5. AUTHORIZATION REGARDING SUB PROCESSORS

5.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) Processor's Affiliates may be retained as Sub-processors; and (b) Processor and Processor's Affiliates may each engage third-party Sub-processors in connection with the provision of the Services.

5.2 **List of Current Sub-processors and Notification of New Sub-processors.**

5.2.1 Processor makes available to Customer the current list of Sub-processors used by Processor to process Personal Data via https://docs.cassiopeia.tech/Privacy%20Policy.pdf. Such Sub-processor list includes the identities of those Sub-processors and the entity's country ("**Sub-Processor List**"). The Sub-Processor List as of the date of first use of the Services by Customer is hereby authorized, and in any event shall be deemed authorized by Customer, unless Customer wish to object to Sub-Processor in accordance with Section 5.3 below.

5.2.2 Processor will notify Customer if it intends to add or replace Sub-processors from the Sub-Processor List at least 10 days prior to any such changes and the Customer will have the right to object to any such appointment in accordance with the said Section 5.3.

5.3 **Objection Right for Proposed Sub-processors.** Customer may reasonably object to Processor's use of existing and/or new Sub-processor ("**Proposed Sub-processor**"), for reasons relating to the protection of Personal Data, by notifying Processor promptly in writing within three (3) business days of first use of the Services and/or receipt of Processor's notice as set out in Section 5.2.2 (as applicable). Such written objection shall include those reasons for objecting to Processor's use of the Proposed Sub-processor. Failure to object in writing within three (3) business days shall be deemed as acceptance of the Proposed Sub-Processor. In the event Customer reasonably objects to a Proposed Sub-processor, as permitted in the preceding sentences, Processor will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or

use of the Services to avoid Processing of Personal Data by the objected-to Proposed Sub-processor without unreasonably burdening the Customer. If Processor is unable to make available such change within thirty (30) days, Customer may, as a sole remedy, terminate the Agreement and this DPA with respect only to those Services which cannot be provided by Processor without the use of the objected-to Proposed Sub-processor, by providing written notice to Processor. All amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Processor. Until a decision is made regarding the Proposed Sub-processor, Processor may temporarily suspend the Processing of the affected Personal Data and/or suspend access to the Services. Customer will have no further claims against Processor due to the termination of the Agreement (including, without limitation, requesting refunds) and/or the DPA in the situation described in this paragraph.

5.4 **Agreements with Sub-processors.** Processor or a Processor's Affiliate has entered into a written agreement with each Sub-processor containing appropriate safeguards to the protection of Personal Data. Where Processor engages a new Sub-processor for carrying out specific Processing activities on behalf of the Customer, the same or materially similar data protection obligations as set out in this DPA shall be imposed on such new Sub-processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR. Where the new Sub-processor fails to fulfil its data protection obligations, Processor shall remain fully liable to the Customer for the performance of the new Sub-processor's obligations.

6. SECURITY

6.1 **Controls for the Protection of Personal Data**. Processor shall maintain industry-standard technical and organizational measures for protection of Personal Data Processed hereunder (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data. Upon the Customer's reasonable request, Processor will assist Customer, at Customer's cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing and the information available to Data Processor.

6.2 **Third-Party Certifications and Audits**. Upon Customer's 14 days prior written request at reasonable intervals (no more than once every 12 months), and subject to strict confidentiality undertakings by Customer, Processor shall make available to Customer that is not a competitor of Processor (or Customer's independent, reputable, third-party auditor that is not a competitor of Processor and not in conflict with Processor, subject to their confidentiality and non-compete undertakings) all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections, conducted by them (provided, however, that such information, audits, inspections and the results therefrom, including the documents reflecting the outcome of the audit and/or the inspections, shall only be used by Customer to assess compliance with this

DPA, and shall not be used for any other purpose or disclosed to any third party without Processor's prior written approval. Upon Processor's first request, Customer shall return all records or documentation in Customer's possession or control provided by Processor in the context of the audit and/or the inspection). Customer shall be fully responsible for bearing all the costs and expenses arising from or related to this Section. If and to the extent that the Standard Contractual Clauses apply, nothing in this Section 6.2 varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

7. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

Processor maintains security incident management policies and procedures and, to the extent required under applicable Data Protection Laws, shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed on behalf of the Customer, including Personal Data transmitted, stored or otherwise Processed by Processor or its Sub Processors of which Processor becomes aware (a "**Personal Data Incident**"). Processor shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Processor deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Processor's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's personnel.

8. RETURN AND DELETION OF PERSONAL DATA

Upon termination of the Agreement and subject thereto, Processor shall, at the choice of Customer (indicated through the Service or in written notification to Processor), delete or return to Customer all the Personal Data it Processes solely on behalf of the Customer in the manner described in the Agreement, and Processor shall delete existing copies of such Personal Data unless Data Protection Laws require or authorize the storage of the Personal Data. To the extent authorized or required by applicable law, Processor may also retain one copy of the Personal Data solely for evidence purposes and/or for the establishment, exercise or defence of legal claims and/or for compliance with legal obligations.

9. CROSS-BORDER DATA TRANSFERS

9.1 **Transfers from the EEA, Switzerland and the United Kingdom to countries that offer adequate level or data protection**. Personal Data may be transferred from EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) (collectively, "**EEA**") Switzerland and the United Kingdom ("**UK**") to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, the Member States or the European Commission ("**Adequacy Decisions**"), without any further safeguard being necessary.

9.2 **Transfers to other countries or entities.** If the Processing of Personal Data by Processor includes transfers (either directly or via onward transfer) from the EEA, Switzerland and/or the UK to countries which have not been subject to an Adequacy Decision, and such transfers are not performed through an alternative

recognized compliance mechanism as may be adopted by Processor for the lawful transfer of personal data (as defined in the GDPR) outside the EEA, Switzerland or the UK, as applicable, then the Standard Contractual Clauses shall apply.

9.3 Where the transfer of Personal Data is made subject to the Standard Contractual Clauses, the "**data importer**" thereunder shall be either the Processor or its Sub-processor, as the case may be and as determined by Processor, and the "**data exporter**" shall be the Controller of such Personal Data. The Processor shall, and shall ensure that the relevant Sub-processor shall (where applicable) comply with the data importer's obligations, and the Controller shall comply with the data exporter obligations, in each case under the applicable Standard Contractual Clauses. If necessary, Processor will ensure that its Sub-processor enters into Standard Contractual Clauses with Customer directly, and in such case Customer hereby gives Processor an instruction and mandate to sign the Standard Contractual Clauses with any such Sub-processor in Customer's name and on behalf of Customer. The Standard Contractual Clauses will not apply to Personal Data that relates to individuals located outside of the EEA, or that is not transferred, either directly or via onward transfer, outside the EEA

10. AUTHORIZED AFFILIATES

10.1 **Contractual Relationship**. The Parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, in which case each Authorized Affiliate agrees to be bound by the Customer's obligations under this DPA, if and to the extent that Customer Processes Personal Data on the behalf of such Authorized Affiliates, thus qualifying them as the "Controller". All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Customer.

10.2 **Communication**. The Customer shall remain responsible for coordinating all communication with Processor under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

11. OTHER PROVISIONS

11.1 **Data Protection Impact Assessment**. Upon Customer's reasonable request, Processor shall provide Customer, at Customer's cost, with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR (as applicable) to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Processor. Processor shall provide, at Customer's cost, reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 11.1, to the extent required under the GDPR.

11.2 **Assistance**. Processor may assist Customer, at Customer's request and cost, in ensuring compliance with Customer's obligations pursuant to the GDPR, CCPA and other applicable Data Protection Laws.

11.3 **Modifications by Customer**. Customer may by at least forty-five (45) calendar days' prior written notice to Processor, request in writing any variations to this DPA if they are required as a result of any change in, or decision of a competent authority under, any Data Protection Laws, to allow Processing of Personal Data to be made (or continue to be made) without breach of that Data Protection Law. Pursuant to such notice: (a) Processor shall make commercially reasonable efforts to accommodate such modification requested by Customer or that Processor believes is necessary; and (b) Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Processor to protect the Processor against additional risks, or to indemnify and compensate Processor for any further steps and costs associated with the variations made herein at Customer's request. The Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable. In the event that the Parties are unable to reach such an agreement within 30 days of such notice, then Customer or Processor may, by written notice to the other Party, with immediate effect, terminate the Agreement to the extent that it relates to the Service which is affected by the proposed variations (or lack thereof). Customer will have no further claims against Processor (including, without limitation, requesting refunds for the Service) pursuant to the termination of the Agreement and the DPA as described in this Section.

11.4 **Modifications by Processor**. Processor may by at least thirty (30) calendar days' prior written notice to Customer, vary the terms of this DPA and/or any Standard Contractual Clauses applicable pursuant to Section 9 of this DPA, as necessary to allow the Processing of Personal Data to be made (or continue to be made) without breach of applicable Data Protection Laws, or to otherwise protect the interests of Processor and/or Customer, in each case as reasonably determined by Processor at its discretion. Customer's continued use of the Service on expiry of the notice period shall signify acceptance of such revised terms. If Customer objects to said variations within the notice period, the Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Processor's notice as soon as is reasonably practicable. In the event that the Parties are unable to reach such an agreement within 30 days of such notice, then Customer or Processor may, by written notice to the other Party, with immediate effect, terminate the Agreement to the extent that it relates to the Service which is affected by the proposed variations (or lack thereof). Customer will have no further claims against Processor (including, without limitation, requesting refunds for the Service) pursuant to the termination of the Agreement and the DPA as described in this Section.

Cassiopeia

ANNEX 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

1. Providing the Services to Customer;
2. Performing the Agreement, this DPA and/or other contracts executed by the Parties;
3. Acting upon Customer's reasonable instructions, where such instructions are consistent with the terms of the Agreement;
4. Providing support and technical maintenance, if agreed in the Agreement;
5. Preventing, mitigating and investigating the risks of data security incidents, fraud, error or any illegal or prohibited activity;
6. Resolving disputes;
7. Enforcing the Agreement, this DPA and/or defending Processor's rights;
8. Complying with applicable laws and regulations;
9. All tasks related with any of the above.

Duration of Processing

Subject to any Section of the DPA and/or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, Processor will Process Personal Data pursuant to the DPA and Agreement for the duration of the Agreement, unless otherwise agreed upon in writing.

Type of Personal Data

Email, First Name, Last Name, Employee Unique ID, Ethnicity Group, Age Group, Employment Status, Marital Status, Gender, Address and any other data which Customer will submit to the Services and which may be linked to individuals.

Categories of Data Subjects

- Employees, agents, advisors, freelancers of Customer (who are natural persons).
- Applicants, prospects, customers, business partners and vendors of Customer (who are natural persons).
- Employees or contact persons of Customer's business partners and vendors.
- Any other third party individual with whom Customer decides to communicate through the Services.