PRIVACY POLICY CEVINIO

Last modified: December 1, 2020

This website (the “Website”) and the Cevinio application (“Cevinio Application”), collectively “Cevinio’ is operated by TBlox B.V. on behalf of ourselves, our group companies, international partnerships and affiliated organizations (“**Cevinio**“, “**we**“, “**our**” or “**us**“).

Your privacy

We recognize that when you choose to provide us with information about yourself, you trust us to act in a responsible manner. This Privacy Notice explains who we are, how we collect, share and use personal information about you, and how you can exercise your privacy rights.

This applies to personal information that we collect through the Website or when engaging in our relationship or potential relationship with you (or your organization) as a supplier, client or business partner.

Our services

There are many different ways you can use our services – to activate and use business application, exchange digital content. When you share information with us, we can make those services even better, to help you connect with business relations or to make sharing information with others quicker and easier. As you use our services, we want you to be clear how we’re using information and the ways in which you can protect your privacy.

Our Privacy Policy explains:

- What information we collect and why we collect it.
- How we use that information.
- The choices we offer, including how to access and update information.

Use of the Cevinio products and services is solely allowed by businesses with a valid company registration number and, if applicable, valid Tax number.

We will process personal data that is stored within Cevinio in accordance with our standard data processing agreement. A signed copy of this agreement is provided on our website. If you are a data controller you can download and cosign this document to meet your statutory personal data protection obligations. When you do so please send us a .pdf copy of the fully signed agreement.

Information we collect

We collect information to provide better services to all of our users – from figuring out basic stuff like which language you select, to more complex things like which apps you'll find most useful.

We collect information in the following ways:

- Information you give us. For example, our services require you to sign up for a Cevinio Account. When you do, we'll ask for personal information, like your name, email address, telephone number.
- Information we get from your use of our services. We collect information about the services that you use and how you use them. This information includes:
  - Log information
  - When you use our services or view content provided by Cevinio, we automatically collect and store certain information in server logs. This includes:
    - details of how you used our service, such as your search queries and what actions you perform.
    - device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
    - cookies that may uniquely identify your browser or your Cevinio Account.
- Location information. When you use Cevinio services, we may collect and process information about your actual location.
- We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.
- Cookies and similar technologies
- We and our partners use various technologies to collect and store information when you visit a Cevinio service, and this may include using cookies or similar technologies to identify your browser or device. We also use these technologies to collect and store information when you interact with services we offer to our partners.
- Information we collect when you are signed in to Cevinio, in addition to information we obtain about you from partners, may be associated with your Cevinio Account. When information is associated with your Cevinio Account, we treat it as personal information.
- We don't collect sensitive personal information

How we use information we collect

We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Cevinio and our users.

We may use the name you provide for your Cevinio Profile across all of the services we offer that require a Cevinio Account. If you have a Cevinio Account, we may display your Profile name, and actions you take on Cevinio or on third-party applications connected to your Cevinio Account.

When you contact Cevinio, we keep a record of your communication to help solve any issues you might be facing. We may use your email address to inform you about our services, such as letting you know about upcoming changes or improvements.

We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. For example, by saving your language preferences, we'll be able to have our services appear in the language you prefer.

We will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy.

Cevinio can processes personal information on our servers in different countries around the world. We may process your personal information on a server located outside the country where you live. We run your data explicitly only in Europe unless requested else by the client. We inform you where your data is located and will not change the location without approval.

Accessing and updating your personal information

Whenever you use our services, we aim to provide you with access to your personal information. If that information is wrong, we strive to give you ways to update it quickly or to delete it – unless we have to keep that information for legitimate business or legal purposes. When updating your personal information, we may ask you to verify your identity before we can act on your request.

We may reject requests that are unreasonably repetitive, require disproportionate technical effort (for example, developing a new system or fundamentally changing an existing practice), risk the privacy of others, or would be extremely impractical (for instance, requests concerning information residing on backup systems).

Where we can provide information access and correction, we will do so for free, except where it would require a disproportionate effort. We aim to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup systems.

Information we share

We do not share personal information with companies, organizations and individuals outside of Cevinio unless one of the following circumstances applies:

- With your consent
- We will share personal information with companies, organizations or individuals outside of Cevinio when we have your consent to do so. We require opt-in consent for the sharing of any sensitive personal information.
- With administrator users of your organization if strictly needed
- If your Cevinio Account is managed for you by a white label version. Your domain administrator may be able to:
    - view statistics regarding your account, like statistics regarding applications you install.
    - suspend or terminate your account access.
    - access or retain information stored as part of your account.
    - receive your account information in order to satisfy applicable law, regulation, legal process or enforceable governmental request.
    - restrict your ability to delete or edit information or privacy settings.
    - please refer to your domain white label privacy policy for more information.
- We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.
- For legal reasons
- We will share personal information with companies, organizations or individuals outside of Cevinio if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:
    - meet any applicable law, regulation, legal process or enforceable governmental request.
    - enforce applicable Terms of Service, including investigation of potential violations.
    - detect, prevent or otherwise address fraud, security or technical issues.
    - protect against harm to the rights, property or safety of Cevinio, our users or the public as required or permitted by law.
- If Cevinio is involved in a merger, acquisition or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

Information security

We work hard to protect Cevinio and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. In particular:

- We encrypt all of our services using SSL.
- We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.
- We restrict access to personal information to Cevinio employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

When this Privacy Policy applies

Our Privacy Policy applies to all of the services offered by Cevinio and its affiliates but excludes services that have separate privacy policies that do not incorporate this Privacy Policy.

Compliance and cooperation with regulatory authorities

Cevinio complies with the General Data Protection Regulation (GDPR) of the EU and in the Netherlands with the Algemene Verordening Gegevensbescherming (AVG). We regularly review compliance with our Privacy Policy. We also adhere to several self regulatory frameworks, including the EU-US Privacy Shield Framework. When we receive formal written complaints, we will contact the person who made the complaint to follow up.

Changes

Our Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any privacy policy changes on this page (**https://www.cevinio.com/user-terms)** and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of privacy policy changes). We will also keep prior versions of this Privacy Policy in an archive for your review.

DATA PROCESSING AGREEMENT CEVINIO

Last modified: December 1, 2020

As per our Privacy Policy we agreed with you that we shall provide you with a standard data processing agreement which shall govern how we process personal data on your behalf. Below you shall find this agreement. It is entered into by Cevinio, Hofplein 20, 3032AC, Rotterdam ("we", "us" or "our" and the legal entity or business which is identified below ("you"). You can accept it by (i) downloading a PDF copy of the **Data Processing Agreement** (our "website") and (ii) returning a fully signed electronic copy by e-mail to us (support@cevinio.com). We will send you a co-signed version back for your files.

1. Definitions
    A. An "Applicable Law" means any legislation applicable to the processing, protection, confidentiality or the privacy of Personal Data.
    B. "Data Processing" means any operation upon the personal data, including without limitation accessing, collecting, storing, using, organizing, combining, altering, transferring, disclosing or deleting the personal data, carried out in the course of our provision of Cevinio to you.
    C. "Disclosure" means any form of disclosure of the Data or any copies thereof to a third party, including, but not limited to, the transfer of data to a third party and the (remote) access to the data by a third party (hereinafter also referred to "Disclose").
    D. "Party" means you or we.
    E. "Parties" means you and we together.
    F. "Personal Data" means information in any form relating to an individual which is processed in the course of our provision of Cevinio to you.
    G. "Third Party" means any party other than the parties to this agreement.
    H. "Transfer" of Personal Data means forwarding, copying and providing remote access to Personal Data (hereinafter also referred to as a verb "Transfers"). "User" means the individual Cevinio user whose personal data is processed in connection with his use of Cevinio.

2. Scope
    A. Our provision of Cevinio to you may involve that we process personal data relating to your users. You agree that we only process personal data: (i) that is created and stored by you as part of your use of the Cevinio platform (like logging details of you actions in the platform) or (ii) subscription information that is displayed in your Cevinio settings. Our obligations as a data processor to you are limited to the personal data we have described in this article 2A.
    B. Any personal data that is included in documents which your users create in Cevinio shall be stored by Amazon Web Services ("AWS") and shall be subject to the applicable AWS privacy policy. You agree that we do not act as data controller nor data processor with respect to this personal data and that AWS shall be solely liable for any damages incurred by you as a result of the processing of such data.

3. Our obligations as a Data Processor
    A. As a data processor we:
        1. shall keep a processing register which contains information (purpose, retention period) about the personal data we process.
        2. shall conduct the data processing in accordance with the applicable law, this agreement and all further reasonable commercial instructions you provide to us with regard to the data processing;
        3. shall perform the data processing appropriately and accurately and only insofar as needed to provide you with Cevinio; and shall not process personal data for purposes not authorized by you;
        4. shall ensure that only our personnel (including the personnel of our hosting party) to the extent required to provide you with Cevinio and enabling us to meet our obligations pursuant to this agreement shall have access to Personal Data and shall require such personnel to protect and maintain the confidentiality and the security of personal data;
        5. shall implement the technical and organizational security measures, as specified in Appendix 1, to protect personal data against unauthorized or unlawful processing, accidental or unlawful destruction or accidental loss, alteration, damage, unauthorized disclosure or unauthorized access by any person;
        6. shall not disclose personal data to any third party without your prior written approval except if this is our hosting party or if our disclosure is obligated by applicable mandatory law, for example after having been issued with a warrant from a competent law enforcement agency;
        7. shall cooperate with you to address and resolve any complaints, requests or inquiries from users, as well as to address any investigations, inspections or audits by any public authority into your practices with respect to data processing.
    B. We shall maintain in place procedures to enable compliance with requests for information by users. All such requests shall be answered within four (4) weeks or as may be required by local law after receipt of the request.
    C. If you require so and provided you notify us well in advance, we shall cooperate with you to perform any risk assessments or audits with regard to the data processing, and shall in particular:
        1. provide you with access to any information which may be reasonably necessary to review our hosting facilities, procedures and documentation relating to the data processing; and
        2. enable you to have an audit executed by a registered IT auditor in accordance with article 7 below.
    D. If our hosting party notifies us of a suspected security incident involving personal data we shall inform you immediately after having received this

information by sending you an e-mail. This email shall include the information that we have received from our hosting provider.

E. According to the GDPR we must report a serious data breach immediately to the local Data Protection Authority. In case of a high risk data breach, we will also report the data breach to the data subject (the person whose personal data has been leaked).
F. We shall not keep personal data any longer than necessary for the purpose of providing you with Cevinio. Subject to our legal and regulatory obligations with regard to personal data we shall ensure that we and our hosting provider, when your subscription for Cevinio ends, shall return all personal data to you by providing you with a copy of the database server table with your Cevinio data. When we have done so we shall be responsible for destroying all personal data related to your users that it in our possession or in the possession of our hosting provider. Subject to the provisions of this article, you hereby authorize and, where relevant, hereby instruct us to:
    1. to disclose personal data to our current hosting provider; and
    2. to disclose personal data to a third party in order to comply with a legal obligation to which you, we or the user are subject, provided such disclosure is directly related to the services provided under this agreement.

4. Your obligations as a Data Controller

As a data controller you:

1. shall provide us with specific written instructions with regard to the security and confidentiality of personal data in accordance with applicable data protection legislation;
2. shall inform us of any legitimate inspection or audit of the data processing by any competent authority which relates to our data processing; and
3. shall inform us as soon as reasonably possible of any access request, request for correction or blocking of personal data or any objection related to our data processing.

5. Liability

A. Parties to indemnify and hold each other, their representatives and employees harmless against any direct and substantiated losses, agreed fees, penalties, fines, direct claims, direct damages, direct, reasonable and substantiated costs and direct, reasonable out-of-pocket expenses (including external legal fees), and other direct and substantiated liabilities they have actually suffered as a result of the other party's material breach of any representations and warranties contained in this agreement, any data protection obligations or laws in any jurisdiction.
B. Our liability is limited to the maximum amount offered pursuant to the Terms & Conditions that applies to your agreement.

6. Terms and termination
    A. This agreement shall be effective for the duration of your agreement for Cevinio unless terminated by either party in accordance with the terms and conditions of this agreement.
    B. Upon termination or receipt of notice of termination of this agreement, we shall as soon as reasonably possible act in accordance with article 3E above.
    C. If a party has not remedied any material breach of this agreement notified to it by the other party within ten (10) days after receipt of such notice, the other party is entitled to terminate this agreement by notice to the failing party without prejudice to any other rights accruing under this agreement or in law.
    D. This agreement may be terminated by the other party in the event that either party:
        1. shall or can reasonably be expected to cease business in the ordinary course;
        2. becomes insolvent;
        3. makes a general assignment for the benefit of its creditors;
        4. suffers or permits the appointment of a receiver or a manager for its business assets; or
        5. avails itself or becomes subject to any proceeding under bankruptcy laws or any other statutes or laws relating to insolvency or protection of the rights of creditors.

7. Audit
    A. For the duration of this agreement and with a maximum frequency of once per calendar year you shall be entitled to have a registered IT auditor verify our compliance with the terms of this agreement and with any legislative, judicial and regulatory provision to which you and your organization are subject to (“audit”). To enable an audit we shall allow this IT auditor access to: (i) our hosting facilities, (ii) our personnel and (iii) our written policies, procedures, processes and controls.
    B. Our obligation to cooperate with your audit is limited to applying our commercially reasonable effort and is subject to compliance by you your IT auditor with the access policies of our hosting provider.
    C. You shall give at least 14 days notice of an audit.
    D. Any audit shall not disrupt unreasonably disrupt our business operations.
    E. Promptly after the issuance of any audit report or findings, you and we shall meet to review the audit report and the findings. We shall consequently at our own expense, undertake reasonable all commercial reasonable remedial action to address and resolve any material deficiencies arising out of any audit.
    F. You shall be responsible for the cost of the audit. If and to the extent the audit report identifies any material deficiencies, we shall only be required to meet our obligations pursuant to article 7E. We shall not be required to pay you any related damages, including but not limited to the audit costs.

8. Governing Law
    A. This agreement is governed by and construed in accordance with the laws of the Netherlands.
    B. Any disputes arising out of, or in connection with this agreement shall be settled by the competent courts in the legal district of Rotterdam.

9. Miscellaneous
    A. Force Majeure
        1. In the event of a Force Majeure situation (as defined hereinafter) the party being delayed shall inform the other party as soon as possible but in any event within three (3) days after the commencement of such Force Majeure situation specifying the nature of the Force Majeure situation as well as the estimated duration thereof. In the event the Force Majeure situation continues for a period of more than thirty (30) days, then either party is entitled to terminate this agreement together with the Terms & Conditions for the agreement for Cevinio by simple notice in writing and without either party being liable for damages towards the other party. If the affected party does not wish to terminate this agreement in accordance with the above, the respective parties' rights and obligations shall be suspended and a new time schedule shall be agreed upon between the parties.
        2. "Force Majeure" shall be understood to mean and include damage or delay caused by unavailability of telecommunications connections and underlying infrastructure, acts or regulations or decrees of any government (de facto or de jure) natural phenomena such as earthquakes and floods, fires, riots, wars, freight embargoes, lockouts or other causes whether similar or dissimilar to those enumerated above unforeseeable and beyond the reasonable control of the pertaining parties and which prevent the total or partial carrying out of any obligation pursuant to this Agreement.

    B. Listing of Annexes
        1. Annex 1 shall be deemed to form, be read and construed as an integral part of this agreement. If any conflict appears between the terms and conditions of the body of this agreement and any of the above documents, the terms and conditions contained in the body of this agreement shall prevail.

As signed in duplicate on the dates identified below:

Data Processor	Data Controller:
By: Cevinio	By:
Name: Vilayat William	Name:
Position: CEO	Position:
Date: November 20, 2020	Date:

Appendix 1 Technical and Organizational Measures

Pursuant to article 3.A.4. of this agreement, we shall:

1. adopt and implement policies and standards related to information security;
2. assign responsibility for information security management;
3. devote adequate personnel resources to information security;
4. perform background checks on permanent staff that shall have access to personal data (where practicable and lawful in each relevant jurisdiction);
5. require our employees, vendors and others to abide by our information security standards and other privacy policies (as such may be revised from time to time), which standards and policies may include confidentiality provisions;
6. conduct training to make employees aware of information security risks and to enhance compliance with our policies and standards relating to data protection;
7. have procedures in place in an attempt to prevent unauthorized access to personal data through the use, as appropriate, of physical and logical (password) entry controls, secure areas for processing and built in system audit trails;
8. protect personal information maintained in online systems through the use, as appropriate, of secure passwords, network intrusion detection technology, encryption and authentication technology, secure log on procedures, and virus protection;
9. ensure compliance with our policies and standards related to data protection on an ongoing basis.