Privacy Statement of MicroHarvest

This Privacy Statement informs you about the processing of your personal data when you visit the MicroHarvest website, communicate with us via email, act as representative for a company that does business with us, or apply for a job with MicroHarvest.

Controller

MicroHarvest is the controller of the processing operations described in this Privacy Statement, except where otherwise indicated for a specific processing operation. This is where we are:

MicroHarvest GmbH

Registered in the Hamburg register of companies under: **HRB168858**

Germany office:	*Portugal office:*
Kasernenstrasse 12	Avenida Infante Dom Henrique 143
21073 Hamburg	Unit N.04
	1950-406 Lisbon

Purposes of processing

MicroHarvest may process your personal data for the following purposes:

- To enable the use and basic security of our website;
- To examine how our website is being used, so that we can make improvements where necessary;
- To communicate with you if you contact us;
- To document the agreements and arrangements we made with you;
- To keep records of business transactions in our financial administration;
- To be able to inform you about our business and about products that we offer;
- To evaluate and respond to your job application;
- To be able to transfer our company (including goodwill / customer base) in case of a merger, a takeover or relaunch.

Legal grounds for processing and retention periods

Processing operations that are necessary for what you are asking of us

If you are visiting our website, email us with a question or apply for a job with us, there are certain personal data that we need to process about you, in order to be able to respond. These are processing operations that we do on the grounds of Article 6 Paragraph 1 (b) of the GDPR.

If you visit our website, we process:

- Information from your device: your computer's IP address, device type, dates and times of visiting the website, activity on the websites and referring websites or applications, uniform resource locators or URLs (i.e. website addresses) visited prior to arriving and after leaving our website and approximate geolocation
- Marketing Preferences including any consents
- Demographic information such as country of residence, gender and age
- Service Engagement such as activities on the Websites

If you reach out to us with questions, comments or requests:

- Name
- Your contact details (according to your choice of communication channel)
- Your communications with us

If you apply for a job with us:

- Name
- Contact details
- Curriculum vitae
- Description of the job that you are interested in and why you are a good match

Providing us with these personal data is a prerequisite for entering into a contract with us, within the meaning of in Article 13 (2) (e) of the GDPR. We cannot show you our website, communicate with you or consider you for a job without processing these personal data.

Retention periods

Website data: Google Analytics keeps your data for up to two months

Communications: We save these until they are no longer relevant. When that is, exactly, depends on the subject of the communications. If communications have a legal or financial component, we may be obliged by law to keep them in our records for 10 years after the communications lose their topicality.

Job applications: How long we save your job application data, depends on whether you come to work with us. If you become part of the team, we will transfer most of the application information to your personnel file and save them there. If we can't hire you, then the retention period depends on your preferences. If you would like to be considered for future vacancies, we can keep your application on file (until you ask us to delete). If you prefer us to delete it right away, we will do that.

In some cases, we may retain the personal data that we mentioned above for a longer period. This is the case if we have reason to believe that retaining the data is necessary for the protection of our legal position in case of a dispute, or if we are required by law to retain certain data for a longer period. For more information about longer retention of personal data in such cases, please refer to the paragraph about 'legitimate interest' in this privacy statement.

Processing operations that we are legally obliged to carry out

These are the personal data that we must process in order to comply with legal obligations that apply to us (Art. 6 (1)(c) GDPR):

- The personal data contained in our financial records, for instance:
    - Name, address, city and country of residence of our customer;
    - The amounts we charged to our customer;
    - The dates on which we have charged amounts to our customer;
    - The type of products or services to which the amounts charged relate, so that the correct VAT rate can be determined;
    - Contact details of the representatives of our customers;
    - Communications and agreements that pertain to sale of products or services.

The retention period for the personal data we process for our financial administration is: ten (10) years after the data has lost its topicality. This means that billing data is destroyed in the eleventh fiscal year after the billing has taken place. If we have an ongoing contract with you or your company, under which we charge, we will retain a copy of that contract for our tax data retention obligations for ten years after the contract ends.

Processing operations that are necessary for a legitimate interest

Sometimes we may process personal data of our own accord, if it is necessary for a legitimate interest of MicroHarvest or of a third party (Art. 6 (1)(f) GDPR).

Personal communication

If we have your contact details, and we have news that we think might be interesting to you, we may decide to drop you an email or give you a call. We do this only in individual cases, when we truly believe that our communication will be of value to you.

We will *not* approach you with unsolicited marketing stuff. If we want to send more general newsletters and things like that, we will do that only on the basis of opt-in consent.

Job application

If you apply for a job with us, we may supplement the information that you send us by looking you up on the internet. This is what we may look at:

- Your profile(s) on professional networking sites (e.g. LinkedIn)
- Articles and other professional writings you may have published
- Whatever you choose to show publicly on other types of networking sites (e.g. Facebook)
- News items about you on the internet, in so far as they are relevant to assessing your fitness for a job with us

We may look at your online networking profiles or news items about you on the internet, but we will not store them in our own computer system. If you published an interesting academic paper, or other writings that we would like to discuss with you in the job application process, we might download them to include them in your application file. The retention period for such data is: until the job application process is finished, unless you would like us to save it for longer.

Legal dispute

If we have any kind of legal relationship with you – for example: if we have done business with you, or if you had an internship or an employment agreement with us – we can decide to retain information about our relationship with you (including personal data) if we have reason to believe that this information may be important to our legal position in the context of a dispute or impending dispute, or if the information may otherwise be necessary for the protection of our legal position.

The retention period for these data is: until our legal relationship with you and/or the dispute over it has been fully settled.

Website analysis

We may use analytical tools to get a general idea of how much interest there is for our website and how we may improve it. Our website monitors the number of people visiting, certain session statistics and a rough approximation of the geographic region from where people are visiting. Analytics tools use personal data like IP address to be able to count the number of (unique) visitors. We will not try to trace website usage data to you personally - unless it looks like your computer is maliciously attacking our website.

Anonymizing data for business intelligence

MicroHarvest wouldn't be the vibrant company it is if we didn't strive to learn from what we are doing every day. Not only in the lab, but in the office as well. We may use facts arising from communications or business that we've done with you to analyze how our business is doing or how our market surroundings are developing. Before we do that, we will first anonymize the data by removing names and other identifying details and using the remaining (non-personal) information in aggregate form.

Processing operations that we do on the basis of your consent

Some processing activities we will only do if you give us permission to do so. For instance:

- Put your contact details on a mailing list for general (non-personal) newsletters or other mailings;
- Have our website place cookies for tracking or marketing, or cookies that share data with recipients outside the EEA;
- Keep your application data on file after the end of a job application procedure;
- Publish pictures you've taken with us (e.g. on a business event) to anybody who wasn't at the event themselves.

The retention period for data processed with your consent is (at the longest) until you withdraw your consent. But we will keep an eye on the relevance of our databases as well. If we have reason to believe that hanging on to your personal data is not useful anymore – neither for us, nor for you – then we may delete it on our own initiative.

Sharing of personal data

We may share your personal data with third parties in the following cases:

Data sharing with processors

For some parts of our business activities, we use service providers outside our own organization. If these service providers process personal data for us, they are – in the terms of the GDPR - our "processors". In such cases, we conclude a processor's agreement with them, as referred to in article 28 paragraph 3 GDPR.

We use the following types of processors:

- A provider of software-as-a-service and cloud storage for our email and general office work;
- Providers of cloud-based collaboration software for our intranet / company wiki's and electronic lab notebook;
- A provider of an HR platform for keeping track of remuneration, social security and other files regarding our employees;
- Providers of cloud-based tools for reimbursement of work-related costs and organizing extra benefits for our employees;
- Social networking media and a webhosting service for presenting our company online.

USA-based processors

We chose our processors with care, paying particular attention to data security. We selected providers who help us process personal data within the EEA as much as possible. Nevertheless, it must be noted that most of our processors are based in the USA or have parent companies in the USA. Our processor's agreements with these processors include the Standard Contractual Clauses most recently ratified by the European Commission, in order to safeguard your privacy when we transfer personal data to these processors.

The Standard Contractual Clauses in themselves cannot always prevent that the USA government may take access to personal data processed by companies who are subject to legislation like the CLOUD Act and/or FISA 702. Before contracting with our processors, we assessed the risk of USA legislation being used to access personal data that we might store with them, and we concluded that the risk is small enough to decide to use these processors. Nevertheless, we want to warn you: if it is very important to you that there is zero risk of your personal data being involved in surveillance or investigative actions by the USA government, you should refrain from applying for a job with us or otherwise sending us your personal data.

Direct contact with processors

In rare cases, it may happen that a processor collects personal data directly from data subjects on our behalf. In such cases, we instruct our processor to collect only the personal data that is necessary for the provision of the services we have agreed with that processor. If you provide additional personal data to one of our processors (more than is necessary for the service they provide to us), please be aware that you do so of your own volition; in such a case, we are not the controller of those additional personal data.

Data sharing based on a legal obligation

Sometimes we are obliged by law to share your personal data with third parties. For example:

- If the police or any other investigative service, the tax authority, a governmental body or any other authority lawfully request personal data from us;
- If a private party has a legitimate claim to receive or access your personal data on the basis of a judicial authorization.

If we receive a request from third party to share your personal data with them, we will inform you of this, unless informing you is not permitted by law.

Data sharing on the basis of a legitimate interest

- *Security and our legal interests*

We may share your personal data with third parties such as our accountant, lawyer and/or a bailiff, a detective agency, cyber security experts or other types of researchers and/or the police if this is reasonably necessary:

- to keep our financial and fiscal records in accordance with the law;
- to protect rights, property or the safety of our organization, our employees, our customers or the public;
- to protect our organization, our employees, our customers or the public from fraudulent or otherwise unlawful, inappropriate or offensive use of our products, our property or our services;
- to respond to a (current or imminent) liability or other (current or imminent) legal consequences.

If we share your personal data on this basis, we will inform you about it if we can. We cannot inform you about sharing your personal data if doing so might interfere with the purpose and effectiveness of the investigation or other measures for which we have to share the data.

- *Financing, sale or merger of our company*

We may share your personal data with third parties if we intend to attract financing for our company, sell our company or a division within our company (either as part of a relaunch or otherwise), or if our company intends to merge with another. In the preparatory phase of a financing agreement, sale or merger, we may share your personal data with potential investors, buyers or merger partners. In this preparatory phase, we will try to anonymize the personal data that are part of our business information as much as possible. When the company is actually transferred (or merged), we will share your personal data with the final buyer or merger partner.

We will not sell your personal data separately - outside of the context of a relaunch, company sale or merger - to an organization that will use your personal data for activities that are significantly different from ours.

If we intend to transfer your personal data to a third party in the course of a relaunch, company sale or merger, we will inform you about this as soon as we can do so without disrupting the preparatory phase of the relaunch, sale or merger.

If we share your personal data with a third party on the basis of a legitimate interest, and the third party is not already appropriately bound to confidentiality by law or by professional deontology, we will conclude a confidentiality agreement with the third party before we share the personal data.

Automatic decision-making and/or profiling

MicroHarvest does not make use of automated decision-making or profiling that will produce any legal effects or that might otherwise significantly affect you. Please note that if you consent to the use of tracking and marketing cookies on our website, some profiling may happen for the purpose of personalizing content to your preferences.

Also, please be aware that if you visit our pages on networking media (LinkedIn, Facebook or such), those media may take their own actions to track you and perhaps engage in profiling. Such actions are not in our control. Please inform yourself about the privacy policy of any third party media where you may want to look us up.

Job applicants

If you want to apply for a job with MicroHarvest, you are always welcome to just email us and send us your application directly. If you do that, your application will be handled entirely and exclusively by humans.

In future, we may decide to implement software tools to modernize the application process. Or perhaps we may advertise job openings on websites or other third party media with built-in application tools. If you apply for a job at MicroHarvest though an app, a tool or a third party website or medium, please read the specific privacy statement for that particular app, tool, website or medium, to see how your personal data will be handled and to see whether any automated decision-making or profiling may happen.

You always have the right to have an automated decision about you reviewed by a human being. If you have any questions about the way your personal data will be (or have been) handled in the course of a job application with us, please contact us via dataprotection@microharvest.com.

Transfer of personal data outside the European Economic Area (EEA)

We process personal data within the EEA as much as we can. Even when we use processors who are based outside of the EEA, we choose regionalized settings to keep our data on servers in the EEA wherever we can. If we have to process personal data outside the EEA, we will try to this in a country that offers an adequate level of personal data protection within the meaning of Article 45 GDPR.

If we would ever need to process personal data in a country that is not covered by an adequacy decision within the meaning of Article 45 GDPR, we will make use of standard contractual clauses made or ratified by the European Commission (within the meaning of Article 46 paragraph 2 under c and d), to ensure that our processor offers adequate safeguards for your privacy. We already explained this further in the paragraph about sharing your personal data with our processors.

If you send personal data to MicroHarvest, or if you decide to come and work with us, please note that we have processors in the following countries outside the EEA:

- USA
- Australia

Third party websites and services

Our website may link to websites of other companies, or include links to online services by other parties. If you decide to visit websites or services by other companies, the data processing policies of that other company applies. MicroHarvest is not the controller for personal data processed by third party websites or services. Be sure to inform yourself about the applicable data processing policies on such websites or services before you decide to provide your personal data through them.

MicroHarvest is active on certain social media, like Facebook and LinkedIn. If you visit our pages there, or contact us through such media, the companies behind those media may also process certain information about you. MicroHarvest is not the controller for personal data processed by such social media. Please be sure to inform yourself about the applicable data processing policies on social media before you use them to visit or contact us.

Security of your personal data

MicroHarvest takes the appropriate technical and organizational measures to secure your personal data. We will ensure that our measures are appropriately updated to remain in line with the state of the art regarding data security. Currently, we apply (at least) the following types of security measures:

- We have taken physical measures in our business premises to ensure that unauthorized persons cannot access our documents, workstations and servers.
- Our company regulations contain behavioral rules to prevent unauthorized access to and/or loss of personal data.
- All our employees are contractually bound to confidentiality.
- We use SSL (Secure Socket Layer) technology where appropriate to encrypt sensitive information and personal data (such as account passwords and other identifying information) during transmission.
- Sensitive information is stored in encrypted form, in so far as is reasonably possible within our company's activities.
- Back-ups of personal data are made to the reasonably possible extent.
- Vulnerabilities in our software are always addressed as quickly as possible.

Insofar as we use the services of third parties, who act on our behalf as processors of personal data, these processors are contractually obliged to take appropriate technical and organizational measures to protect the personal data.

Although we do our best to ensure good security, we must point out that absolute security when storing personal data and sending data over the Internet can never be guaranteed.

Your rights

For all processing operations that we carry out on the basis of your consent, you have the right to withdraw your consent at any time. We will then discontinue the processing operations in question. Please note that the processing operations that already took place on the basis of your granted consent will not become unlawful with retroactive effect.

You have the right to object against processing operations that we carry out on the basis of a legitimate interest, on grounds relating to your particular situation.

In all cases, you have the right to request access to the personal data we process about you, the right to have inaccuracies in your personal data corrected ('right to rectification') and the right to have your personal data erased if their processing is not/no longer based on a valid legal ground.

If there is no longer a valid legal ground for our processing of your personal data, but you do not want to have the data removed immediately, you can also make use of the right to 'restriction of processing'. Restriction of processing means that we retain your personal data for you, but do not use it for any other purpose.

In some cases, you may have the right to data portability. Data portability means that you can receive your personal data from us in a structured, commonly used and machine-readable format, or have it transferred to a new service provider (where technically feasible). This right only applies to personal data that you have provided directly to us and that we process on the basis of your consent, or because it is necessary for the performance of our contract with you.

To exercise your rights, please contact us using the contact details stated at the end of this Privacy Statement.

Your right to lodge a formal complaint

If you are dissatisfied with anything related to our processing of your personal data, please discuss it with us so that we can try to resolve it. You can contact us for this purpose using the contact details below.

If we are unable to resolve your objection within a reasonable period of time, you have the right to lodge a complaint with the supervisory authority for the protection of personal data, either:

- In the EU member state where you live or habitually reside;
- In the EU member state where you work;
- In one of the EU member states where MicroHarvest has its offices (Germany and Portugal).

For more information on how to lodge a complaint in Portugal, click here.

For more information on how to lodge a complaint in (Hamburg) Germany, click here.

Contact us about your privacy

For questions or comments on our processing of personal data, or to exercise your rights, please contact us at:

dataprotection@microharvest.com

Updates to this privacy statement

Our privacy statement may be changed or updated from time to time. We can do this unilaterally, by amending this page.

This page was last updated on 28 September 2023.

Please revisit this page from time to time to stay aware of the most up-to-date version.