Privacy Policy:

anuboXBRL GmbH & Co. KG

I. Name and Address of the Controller

The controller within the meaning of the General Data Protection Regulation and other national data protection laws of the member states as well as other data protection provisions is:

anuboXBRL GmbH & Co. KG
represented by the Managing Director
of anubo Verwaltungs GmbH
Dr. Bodo Kesselmeyer
Stadelbergerstr. 32
82256 Fürstenfeldbruck
Germany
Phone: +49 8141 35758 - 0
Email: privacy@anubo.com
Website: https://anubo.com

II. General Information on Data Processing

1. Scope of the Processing of Personal Data

We generally process personal data of our users only to the extent necessary to provide a functional website as well as our content and services. The processing of personal data of our users takes place regularly only with the consent of the user. An exception applies in such cases where prior consent cannot be obtained for factual reasons and the processing of the data is permitted by legal regulations.

All personal data is stored and processed within the EU/EEA and is subject to EU data protection laws, including the General Data Protection Regulation (GDPR). We do not transfer personal data to countries outside the EU/EEA unless explicitly stated in this Privacy Policy (e.g., when using specific third-party services that may process data outside the EU).

We implement appropriate technical and organizational measures to ensure the security of your personal data, including encryption, access controls, and regular security assessments.

2. Legal Basis for the Processing of Personal Data

Insofar as we obtain the consent of the data subject for processing operations involving personal data, Art. 6(1)(a) GDPR serves as the legal basis. When processing personal data that is necessary for the performance of a contract to which the data subject is a party, Art. 6(1)(b) GDPR serves as the legal basis. This also applies to processing operations that are necessary to carry out pre-contractual measures.

Insofar as the processing of personal data is necessary for compliance with a legal obligation to which our company is subject, Art. 6(1)(c) GDPR serves as the legal basis. In the event that vital interests of the data subject or another natural person require the processing of personal data, Art. 6(1)(d) GDPR serves as the legal basis.

If processing is necessary to safeguard a legitimate interest of our company or a third party, and the interests, fundamental rights, and freedoms of the data subject do not override the former interest, Art. 6(1)(f) GDPR serves as the legal basis for the processing.

3. Data Deletion and Storage Duration

The personal data of the data subject will be deleted or blocked as soon as the purpose of storage ceases to apply. Storage may also take place if this has been provided for by the European or national legislator in Union regulations, laws, or other provisions to which the controller is subject.

Data will also be blocked or deleted when a storage period prescribed by the aforementioned standards expires, unless there is a necessity for further storage of the data for the conclusion or performance of a contract.

III. Provision of the Website and Creation of Log Files

1. Description and Scope of Data Processing

Each time our website is accessed, our system automatically collects data and information from the computer system of the accessing computer.

The following data is collected:

(1) Information about the browser type and version used

(2) The user's operating system

(3) The user's internet service provider

(4) The user's IP address

(5) Date and time of access

(6) Websites from which the user's system accesses our website

(7) Websites that are accessed by the user's system via our website

The data is also stored in the log files of our system. This data is not stored together with other personal data of the user.

2. Legal Basis for Data Processing

The legal basis for the temporary storage of the data and the log files is Art. 6(1)(f) GDPR.

3. Purpose of Data Processing

Temporary storage of the IP address by the system is necessary to enable delivery of the website to the user's computer. For this purpose, the user's IP address must remain stored for the duration of the session.

Storage in log files is carried out to ensure the functionality of the website. In addition, the data serves us to optimize the website and to ensure the security of our information technology systems. An evaluation of the data for marketing purposes does not take place in this context.

These purposes also constitute our legitimate interest in data processing pursuant to Art. 6(1)(f) GDPR.

4. Duration of Storage

The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected. In the case of data collection for the provision of the website, this is the case when the respective session has ended.

In the case of storage of data in log files, this is the case after seven days at the latest. Further storage is possible. In this case, the IP addresses of the users are deleted or anonymized, so that an assignment of the calling client is no longer possible.

5. Objection and Removal Option

The collection of data for the provision of the website and the storage of the data in log files is absolutely necessary for the operation of the website. Consequently, there is no possibility of objection on the part of the user.

IV. Use of Cookies

1. Description and Scope of Data Processing

Our website uses cookies and similar technologies (e.g., local storage) to ensure the site functions properly and to measure usage in aggregated form where you consent. Necessary cookies store, for example, your language and consent choices and are required for the site to operate correctly.

2. Legal Basis for Data Processing

Necessary cookies: Art. 6(1)(f) GDPR (our legitimate interest in a secure and functional website) and, where required to perform a contract, Art. 6(1)(b) GDPR.

Analytics cookies: Art. 6(1)(a) GDPR (consent). Analytics only runs after you grant consent in the cookie banner.

3. Consent Management

We use a consent banner (CookieYes) to collect, store, and honor your choices. You may change or withdraw your consent at any time via “Cookie Settings” (footer link). We also retain a record of your consent decision for compliance purposes.

We retain a record of your consent decision for up to 2 years (or longer if required to demonstrate compliance), after which logs are deleted or anonymized.

4. Duration of Storage, Objection and Removal Option

Cookies are stored in your browser. You can delete them at any time using your browser settings. If you withdraw consent or disable cookies, some site features may no longer be available. Analytics cookies are not set unless and until consent is granted.

V. Links to third-party websites

Our website may contain links to third-party sites. When you follow such links, the processing of your personal data is governed by the privacy policies of those third parties. We are not responsible for their content or practices. We do not transmit your personal data to those sites in connection with a simple outbound link; any collection on the third-party site occurs under that site’s control.

VI. Newsletter

1. Description and Scope of Data Processing

Our website may offer the option to subscribe to a free newsletter. When registering for the newsletter, the data from the input form (the user's email address) is transmitted to us. Additionally, the following data is collected during registration:

- IP address of the requesting computer
- Date and time of registration

During the registration process, your consent is obtained for the processing of your data, and reference is made to this privacy policy.

If you purchase goods or services on our website and provide your email address in the process, this address may subsequently be used by us to send a newsletter. In such a case, the newsletter will only contain direct advertising for our own similar goods or services.

The newsletters are sent via our own server in Bavaria and thus without transferring your email address to third parties. We also intend to continue relying solely on our own mail servers and avoid the use of third-party newsletter providers. Should this no longer be technically or economically feasible in the future, we hereby guarantee that we will only

engage newsletter service providers based within the EU. In any case, your data will be used exclusively for sending the newsletter.

2. Legal Basis for Data Processing

The legal basis for the processing of data after registration for the newsletter, provided consent has been given by the user, is Art. 6(1)(a) GDPR.

The legal basis for sending newsletters following the sale of goods or services is § 7(3) UWG (German Act Against Unfair Competition).

3. Purpose of Data Processing

The user's email address is collected to deliver the newsletter.

Other personal data collected during the registration process is used to prevent misuse of the services or the provided email address.

4. Duration of Storage

The data is deleted as soon as it is no longer necessary to achieve the purpose for which it was collected. Accordingly, the user’s email address is stored as long as the newsletter subscription is active.

Other personal data collected during the registration process is usually deleted after seven days.

The metadata of emails generated by our web server (such as newsletters, notifications during the double opt-in process, etc.) is automatically deleted after six months. Metadata includes the email address, date, and subject line of the email. The contents of the emails are not stored on the web server

5. Objection and Removal Option

Users may cancel their newsletter subscription at any time. A corresponding link is provided in every newsletter.

This also enables users to withdraw their consent to the storage of personal data collected during the registration process.

VII. Registration

1. Description and Scope of Data Processing

On our website, we offer users the opportunity to register by providing personal data. The data is entered into an input mask, transmitted to us, and stored. The data is not shared with third parties.

The following data is collected during the registration process:

(1) User Name

(2) First Name

(3) Last name

(4) Email

(5) Microsoft 365 Account Email (optional; used for automatic sign-in with the Microsoft Excel add-in)

(6) Company Name

(7) Password and Confirm Password (**stored as a salted one-way hash**)

(8) Postal address

(9) Customer category, in particular category in the financial data communication process (e.g., issuer, agency, auditing firm, software manufacturer, authority, investment professional, service provider, etc.)

(10) Telephone number

Technical metadata (for security/abuse prevention):
IP address, date and time of registration

As part of the registration process, the user's consent to the processing of this data is obtained.

2. Legal Basis for Data Processing

The legal basis for processing the data, if the user has given their consent, is Art. 6 (1) (a) GDPR.

The legal basis for processing the data transmitted when sending an email is Art. 6 (1) (f) GDPR. If the email contact is aimed at concluding a contract, an additional legal basis for processing is Art. 6 (1) (b) GDPR.

3. Purpose of Data Processing

User registration may be required for:

(1) the provision of Software as a Service (SAAS), such as add-ins for Microsoft software products.

(2) the provision of specific content and services, such as

(3) product information tailored to a specific customer group and/or specific offers.

(4) the sending of the information you request by email or post.

(5) contacting customer support via email, post, or telephone (orders, order processing, billing, etc.).

(6) a web forum for software support.

(7) product support via email or telephone.

Alternatively, user registration may be required to fulfill a contract with the user or to carry out pre-contractual measures. For example, for certain product variants, it must be ensured that contracts are only concluded with users of the target customer group.

4. Duration of Storage

The data is deleted as soon as it is no longer necessary to achieve the purpose for which it was collected. This is the case for the data collected during the registration process if the registration on our website is canceled or modified.

In the case of a registration process for the fulfillment of a contract or for the implementation of pre-contractual measures, the data will be deleted when the data is no longer required for the execution of the contract. Even after the conclusion of the contract, it may be necessary to store the contractual partner's personal data in order to comply with contractual or legal obligations.

5. Objection and Removal Option

As a user, you have the option to cancel your registration at any time. You can have the data stored about you changed at any time. You can initiate the change or deletion of data yourself after logging in to our website.

If the data is required to fulfill a contract or to carry out pre-contractual measures, premature deletion of the data is only possible if contractual or legal obligations do not prevent deletion.

VIII. Contact form and email contact

1. Description and Scope of Data Processing

Our website may contain a contact form that can be used for electronic contact. If a user uses this option, the data entered in the input mask will be transmitted to us and stored. This data includes:

- Reason for interest (e.g., product purchase, partnership, press, event organizer, supplier, potential employee)
- anubo product name and version (if applicable)
- Company, if applicable
- anubo customer number, if applicable
- User name
- Email
- Telephone
- Free communication

The following data is also stored when the message is sent:

- The user's IP address
- Date and time
- Page URL
- User agent - technical data on the operating system, browser version, etc.

Your consent to the processing of the data will be obtained during the sending process, and reference will be made to this privacy policy.

Alternatively, you can contact us via the provided email address. In this case, the user's personal data transmitted with the email will be stored.

The data will not be passed on to third parties in this context. The data will be used exclusively for processing the conversation.

2. Legal Basis for Data Processing

Where the user has given consent, the legal basis is Art. 6(1)(a) GDPR.

The legal basis for processing data transmitted in the course of sending an email is Art. 6(1)(f) GDPR (our legitimate interest in handling inquiries). If the email contact aims to conclude a contract, the additional legal basis is Art. 6(1)(b) GDPR.

3. Purpose of Data Processing

The processing of the personal data from the input mask serves us solely to process the contact. In the case of contact via email, this also constitutes the necessary legitimate

interest in processing the data. The other personal data processed during the sending process serves to prevent misuse of the contact form and to ensure the security of our information technology systems.

4. Duration of Storage

The data will be deleted as soon as it is no longer required to achieve the purpose for which it was collected. For personal data from the contact form input mask and those sent via email, this is the case when the respective conversation with the user has ended. The conversation is concluded when it can be inferred from the circumstances that the matter in question has been conclusively clarified.

The metadata of the emails created by our web server (e.g., with the data from the contact form) is automatically deleted after 6 months. This metadata includes the email address, date, and subject of the email. The content of the emails, i.e., the data from the contact form, is not stored on the web server.

5. Objection and Removal Option

The user has the right to withdraw their consent to the processing of personal data at any time. If the user contacts us by email, they can withdraw their consent to the storage of their personal data at any time. In such a case, the conversation cannot be continued.

Please send your withdrawal of consent and objection to storage to: anubo Verwaltungs GmbH, Data Protection, Stadelbergerstr. 32, D-82256 Fürstenfeldbruck, or by email to privacy@anubo.com. In this case, all personal data stored during the contact process will be deleted.

IX. Security Measures and Third-Party Components

1. Two-Factor Authentication (TOTP)

a) Description and Scope of Data Processing

We offer two-factor authentication (2FA) using Time-based One-Time Password (TOTP) to enhance the security of your account. When you enable TOTP, we generate and store an encrypted shared secret on our servers. This secret is used to verify time-based authentication codes generated by your authenticator app (e.g., Microsoft Authenticator, Google Authenticator, 1Password).

The following data is processed:

- Encrypted TOTP secret (stored using Fernet encryption)
- Activation status (is_active)
- Timestamp of TOTP setup (created_at)
- Timestamp of last successful verification (last_verified_at)

The TOTP secret is generated locally on our servers and is immediately encrypted before storage. We do not transmit the secret to third parties. The secret is stored on our application servers hosted in Germany.

b) Legal basis

The legal basis for the processing of TOTP data is Art. 6(1)(f) GDPR (legitimate interest in account security and fraud prevention) and, where applicable, Art. 6(1)(b) GDPR (contract performance for account access).

c) Purpose of Data Processing

OTP is used to:

- Verify your identity during email confirmation
- Provide secure login authentication for our services (Excel Add-in, Forum, etc.)
- Enhance account security by requiring a second authentication factor
- Prevent unauthorized access to your account

d) Duration of Storage

TOTP data is retained for as long as your account is active and TOTP is enabled. You may disable TOTP at any time through your account settings. Upon account deletion, all TOTP data is permanently deleted. If you disable TOTP, the encrypted secret and related timestamps are deleted immediately.

e) Objection and Removal Option

TOTP is an optional security feature. You are not required to enable it. You may disable TOTP at any time through your account settings, which will result in the immediate deletion of your TOTP configuration. If you wish to re-enable TOTP, you will need to set it up again by scanning a new QR code.

f) Data Security

The TOTP secret is encrypted using Fernet symmetric encryption (AES-128 in CBC mode) before storage. The encryption key is stored separately and is not accessible to application code. We do not transmit TOTP secrets to third parties, and all processing occurs on our servers hosted in Germany.

2. Google reCAPTCHA (website security)

a) Description and Scope of Data Processing

We use Google reCAPTCHA to protect our website and email confirmation process from automated abuse, spam, and unauthorized access attempts. reCAPTCHA is provided by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.

We use reCAPTCHA v3 (invisible) for background security checks. If the risk score is too low, Google may automatically switch to reCAPTCHA v2 (challenge-based verification).

When you use features protected by reCAPTCHA (such as email confirmation or form submissions), the following data may be transmitted to Google:

- Your IP address (explicitly sent as `remoteip` parameter during server-side verification)
- Browser type and version
- Operating system information
- Mouse movements, keyboard input patterns, and other interaction data
- Cookies and local storage data
- reCAPTCHA token generated by your browser

The reCAPTCHA verification process works as follows:

1. When you interact with a protected page, Google's reCAPTCHA script runs in the background (v3) or presents a challenge (v2)
2. A token is generated and sent to our server
3. Our server verifies the token with Google's API (`https://www.google.com/recaptcha/api/siteverify`)
4. For v3, we check the risk score (minimum 0.5) and action type
5. Access is granted or denied based on the verification result

b) Legal basis

Art. 6(1)(f) GDPR (legitimate interest in security, fraud prevention, and protection against automated abuse). Where applicable in the EEA, we load reCAPTCHA only when needed (e.g., upon form submission) and honor your cookie choices. Google provides GDPR commitments for reCAPTCHA as part of Google Cloud’s data processing terms.

c) Purpose of Data Processing

reCAPTCHA is used to:

- Protect our website and services from automated abuse and spam
- Secure the email confirmation process against unauthorized access
- Prevent automated account creation and form submissions
- Enhance overall security of our platform

d) Duration of Storage

reCAPTCHA tokens are temporary and are only used for the immediate verification process. We do not store reCAPTCHA tokens on our servers. Google may store data according to its

own privacy policy. For details, see Google's Privacy Policy:
https://policies.google.com/privacy

e) Objection and Removal Option

The use of reCAPTCHA is necessary for the security of our services. If you do not wish to use reCAPTCHA, you may choose alternative authentication methods (such as TOTP) where available. However, some features may not be accessible without completing reCAPTCHA verification.

You can find more information about Google reCAPTCHA and Google's privacy practices at:

- Google Privacy Policy: https://policies.google.com/privacy
- Google Terms of Service: https://policies.google.com/terms

3. Google Analytics 4 ("GA4")

a) Scope of processing of personal data

If you consent to Analytics in the cookie banner, GA4 collects event data about how the website is used (e.g., page URLs, referrers, basic device information, approximate region). GA4 does not log or store individual IP addresses; for EEA users, Google states that IP addresses are discarded prior to logging

b) Legal basis for the processing of personal data

Art. 6(1)(a) GDPR (consent).

c) Purpose of data processing

To understand aggregated usage and improve content and website performance. We do not enable Google Signals, demographics, Ads linking, or remarketing features.

d) Consent Mode

We use Google's Consent Mode to ensure that GA4 behaves according to your choice (e.g., analytics_storage denied or granted). When consent is denied, GA4 will not read/write analytics cookies; only limited cookieless pings for basic, aggregated measurement may be sent.

e) International transfers and safeguards

Where Google services involve transfers to the U.S., Google participates in the EU–U.S. Data Privacy Framework; see Google's DPF notice and certification.

f) Objection and removal

You can withdraw your analytics consent at any time via “Cookie Settings” with effect for the future.

4. Google Tag Manager (“GTM”)

a) Scope of processing of personal data

GTM is a tag-loading tool. GTM itself does not use its own cookies and does not access personal data; it only deploys other tags, which run according to the consent you choose in the banner. For tags that require consent (e.g., analytics), the legal basis is Art. 6(1)(a) GDPR; for the necessary operation of GTM, Art. 6(1)(f) GDPR (our legitimate interest in a functional website).

b) Legal basis

For tags that require consent (e.g., analytics): Art. 6(1)(a) GDPR. Necessary operational use of GTM to load essential scripts: Art. 6(1)(f) GDPR.

5. Embedded media and social widgets (Vimeo, Twitter/X, LinkedIn)

a) Scope of processing of personal data

We may embed third-party content. We load these embeds only after you enable the relevant category in Cookie Settings. When enabled, the provider may receive your IP address, URL, and browser data and may set cookies.

- Vimeo player may set vuid (analytics for the video owner; typical expiration 2 years) and a player preference cookie. See Vimeo’s cookie and privacy notices.
- Twitter/X and LinkedIn widgets may set cookies or use similar technologies per their policies.

b) Legal basis

Art. 6(1)(a) GDPR (consent). You can enable/disable these embeds via **Cookie Settings** at any time.

X. Rights of the Data Subject

If your personal data is processed, you are a data subject within the meaning of the GDPR and you have the following rights vis-à-vis the controller:

1. Right to information

You can request confirmation from the controller as to whether personal data concerning you is being processed by us.

If such processing occurs, you can request information from the controller about the following:

(1) the purposes for which the personal data are being processed;

(2) the categories of personal data being processed;

(3) the recipients or categories of recipients to whom the personal data concerning you have been or will be disclosed;

(4) the planned duration of storage of the personal data concerning you or, if specific information is not available, criteria for determining the storage period;

(5) the existence of a right to rectification or erasure of the personal data concerning you, a right to restriction of processing by the controller, or a right to object to such processing;

(6) the existence of a right to lodge a complaint with a supervisory authority;

(7) all available information about the origin of the data if the personal data are not collected from the data subject;

(8) the existence of automated decision-making, including profiling, pursuant to Art. 22 (1) and (4) GDPR and – at least in these cases – meaningful information about the logic involved, as well as the significance and intended consequences of such processing for the data subject.

You have the right to request information about whether the personal data concerning you will be transferred to a third country or to an international organization. In this context, you can request to be informed of the appropriate safeguards pursuant to Art. 46 GDPR in connection with the transfer.

2. Right to rectification

You have the right to have the personal data concerning you rectified and/or completed by the controller if the personal data concerning you that are processed are inaccurate or incomplete. The controller must carry out the rectification immediately.

3. Right to Restriction of Processing

You may request the restriction of the processing of your personal data under the following conditions:

(1) if you contest the accuracy of the personal data concerning you for a period enabling the controller to verify the accuracy of the personal data;

(2) the processing is unlawful and you oppose the erasure of the personal data and instead request the restriction of their use;

(3) the controller no longer needs the personal data for the purposes of the processing, but you require them to assert, exercise, or defend legal claims, or

(4) if you have objected to the processing pursuant to Art. 21 (1) GDPR and it has not yet been determined whether the legitimate reasons of the controller outweigh your reasons.

If the processing of personal data concerning you has been restricted, this data – apart from its storage – may only be processed with your consent or for the establishment, exercise, or defense of legal claims or to protect the rights of another natural or legal person, or for reasons of important public interest of the Union or a Member State.

If the restriction of processing has been restricted in accordance with the above-mentioned conditions, you will be informed by the controller before the restriction is lifted.

4. Right to erasure

a) **Obligation to erase**

You may request the controller to delete the personal data concerning you immediately, and the controller is obliged to delete this data immediately if one of the following reasons applies:

(1) The personal data concerning you are no longer necessary for the purposes for which they were collected or otherwise processed.

(2) You withdraw your consent on which the processing was based pursuant to Art. 6 (1) (a) or Art. 9 (2) (a) GDPR, and there is no other legal basis for the processing.

(3) You object to the processing pursuant to Art. 21 (1) GDPR and there are no overriding legitimate grounds for the processing, or you object to the processing pursuant to Art. 21 (2) GDPR.

(4) The personal data concerning you were processed unlawfully.

(5) The deletion of the personal data concerning you is necessary to fulfill a legal obligation under Union or Member State law to which the controller is subject.

(6) The personal data concerning you were collected in relation to information society services offered in accordance with Article 8 (1) GDPR.

b) **Information to third parties**

If the controller has made the personal data concerning you public and is obliged to erase it pursuant to Art. 17 (1) GDPR, the controller shall take appropriate measures, including technical ones, taking into account the available technology and the implementation costs, to inform data controllers which process the personal data that you, as the data subject,

have requested the erasure of all links to these personal data or of copies or replications of these personal data.

c) **Exceptions**

The right to erasure shall not apply if processing is necessary

(1) for exercising the right to freedom of expression and information;

(2) for compliance with a legal obligation requiring processing by Union or Member State law to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(3) for reasons of public interest in the area of public health pursuant to Article 9 (2) (h) and (i) and Article 9 (3) GDPR;

(4) for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes pursuant to Article 89 (1) GDPR, insofar as the right referred to in section a) is likely to render impossible or seriously compromise the achievement of the objectives of that processing, or

(5) for the establishment, exercise, or defense of legal claims.

5. Right to information

If you have asserted your right to rectification, erasure, or restriction of processing vis-à-vis the controller, the controller is obliged to inform all recipients to whom the personal data concerning you was disclosed of this rectification, erasure, or restriction of processing, unless doing so proves impossible or involves disproportionate effort. You have the right to be informed by the controller of these recipients.

6. Right to data portability

You have the right to receive the personal data concerning you that you have provided to the controller in a structured, common, and machine-readable format. You also have the right to transmit this data to another controller without hindrance from the controller to whom the personal data was provided, provided that

(1) the processing is based on consent pursuant to Art. 6 (1) (a) GDPR or Art. 9 (2) (a) GDPR or on a contract pursuant to Art. 6 (1) (b) GDPR and

(2) the processing is carried out using automated procedures.

In exercising this right, you also have the right to have the personal data concerning you transmitted directly from one controller to another, where technically feasible. The freedoms and rights of others must not be adversely affected.

The right to data portability does not apply to the processing of personal data necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

7. Right of Objection

You have the right to object at any time to the processing of personal data concerning you based on Art. 6 (1) (e) or (f) GDPR, for reasons related to your particular situation; this also applies to profiling based on these provisions.

The controller will no longer process the personal data concerning you unless they can demonstrate compelling legitimate grounds for the processing that override your interests, rights, and freedoms, or the processing serves to assert, exercise, or defend legal claims.
If the personal data concerning you is processed for direct marketing purposes, you have the right to object at any time to the processing of personal data concerning you for the purposes of such advertising; this also applies to profiling insofar as it is related to such direct marketing.

If you object to processing for direct marketing purposes, the personal data concerning you will no longer be processed for these purposes. In connection with the use of information society services, you have the option of exercising your right of objection by means of automated procedures that use technical specifications – notwithstanding Directive 2002/58/EC.

8. Right to withdraw your consent to data protection

You have the right to withdraw your consent to data protection at any time. The withdrawal of consent does not affect the legality of the processing carried out on the basis of the consent until the withdrawal.

9. Additional information for California residents (CPRA)

We do not sell or share your personal information as defined by the California Privacy Rights Act. We process analytics only with your consent and do not use personal information for cross-context behavioral advertising. California residents may exercise their CPRA rights (access, deletion, correction, non-discrimination) by contacting us at privacy@anubo.com or by post at the address listed above. We will verify and respond to requests as required by law.

10. Automated decision-making in individual cases, including profiling

You have the right not to be subjected to a decision based exclusively on automated processing – including profiling – that has legal consequences for you or significantly affects you in a similar way. This does not apply if the decision

(1) is necessary for entering into or fulfilling a contract between you and the controller,

(2) is permitted by Union or Member State law to which the controller is subject, and this law contains appropriate measures to safeguard your rights and freedoms as well as your legitimate interests, or

(3) is made with your explicit consent.

However, these decisions may not be based on special categories of personal data pursuant to Art. 9 (1) GDPR, unless Art. 9 (2) (a) or (g) GDPR applies and appropriate measures to protect your rights and freedoms as well as your legitimate interests have been taken.
With regard to the cases referred to in (1) and (3), the controller shall implement appropriate measures to safeguard your rights and freedoms as well as your legitimate interests, including at least the right to obtain human intervention on the part of the controller, to express his or her point of view, and to contest the decision.

11. Right to lodge a complaint with a supervisory authority

Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, place of work, or place of the alleged infringement, if you believe that the processing of personal data concerning you infringes the GDPR.

The supervisory authority with which the complaint was submitted will inform the complainant of the status and outcome of the complaint, including the possibility of a judicial remedy under Article 78 GDPR.

XI. Use of our Excel Add-in and Microsoft integrations

1. Sign-in with Microsoft (SSO)

Description and scope of data processing. When you sign in to our Excel add-in with your Microsoft 365 account, we receive an identity token from Microsoft that includes **your name, email/user principal name**, and **unique identifiers** such as **user ID (oid)** and **tenant ID (tid).** Where permitted, we may also use Microsoft Graph User.Read to retrieve your basic profile (for example: displayName, givenName, surname, mail, userPrincipalName, id). We do not receive your Microsoft password.

Purposes. Authentication, license assignment, and customer support for the add-in.

Legal basis. Art. 6(1)(b) GDPR (contract performance) and Art. 6(1)(f) GDPR (legitimate interests in security/fraud prevention).

Retention. We keep license-relevant identifiers (e.g., tenant ID, user ID, email) while your account/subscription is active and as required by law thereafter.

Controller roles. Microsoft acts as an independent controller for its identity platform; we process the data we receive under this Policy.

2. Purchases via Microsoft Store/AppSource (transactable SaaS)

Description and scope of data processing. If you acquire a paid edition (of anuboXBRL Analyzer) through Microsoft's commercial marketplace, Microsoft shares subscription details required to provision your service (for example **offer/plan IDs, seat quantity, purchaser/beneficiary email, objectId, tenantId**). **Payment processing is performed by Microsoft; we do not receive card details.** Microsoft may also provide validated **customer leads** (contact information, for example email) when you transact, start a trial, or express interest.

Purposes. Provisioning, entitlement management, customer support, and billing/collections where applicable.

Legal basis. Art. 6(1)(b) GDPR (contract performance) and Art. 6(1)(f) GDPR (legitimate interests in account management and support).

Retention. Subscription/entitlement records are retained for the life of the subscription and statutory retention periods.

3. Data sources

We obtain personal data from: (i) you (forms, support), (ii) Microsoft identity platform for SSO claims and, if granted, Microsoft Graph User.Read profile data, and (iii) Microsoft commercial marketplace (subscription details and validated leads).

anuboXBRL GmbH & Co. KG
Stadelbergerstr. 32
82256 Fürstenfeldbruck
Germany
https://anubo.com