Preamble

Protecting your personal data is very important to us. Therefore we collect, store and process your data exclusively on basis of legal regulations. In this privacy statement, we inform you which personal data we collect, store and process, for what purpose we do this and how long personal data is stored. This privacy statement applies to all processing of personal data on our website and in the context of the provision of our services. The terms used are gender-neutral.

Person in charge (=controller)

Zotter Alexander Karl
Pfitznergasse 37
8053 Graz
Austria
Email: contact@alexander-zotter.at
Phone: +43 670 4081768
Imprint: https://accounda.com/imprint/

If you have any questions about this privacy statement or processing of your data, please contact us: service@accounda.com

Legal bases

Lawfulness of processing

General Data Protection Regulation (GDPR)

Processing [of personal data] shall be lawful only if and to the extent that at least one of the following applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes (Art. 6 Para. 1 S. (a) GDPR)
- processing is necessary for compliance with a legal obligation to which the controller is subject (Art. 6 Para. 1 S. (c) GDPR)
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (Art. 6 Para. 1 S. (f) GDPR)

The above text passages on GDPR were taken from the following source (see in more detail ibid.): https://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1/en/pdf

Although the General Data Protection Regulation is directly applicable as an EU regulation in every EU member state, it contains numerous opening clauses and leaves the national legislator certain leeway

for specific regulations. Consequence of opening clauses is that additional regulations may apply to your country of residence or our country of residence. In case of doubt, Austrian law is considered agreed.

Key Austria-specific regulations

Facilitation of the right of correction and erasure of personal data:

If the correction or erasure of personal data processed by automated means cannot executed immediately (because of economic or technical reasons, this can only be done at certain times) the processing of the personal data concerned must be restricted up to that date.

Restriction on right of information:

The right to information of the person concerned does not exist vis-à-vis a controller (without prejudice to other statutory obligations of secrecy) if the provision of this information would jeopardize a business or trade secret of the controller or third parties.

Data secrecy:

The controller must keep confidential (without prejudice to other statutory obligations of secrecy) personal data resulting from data processing entrusted (or have become accessible) to them. This applies to the extent that there is no legally permissible reason for the transfer of personal data entrusted to us or that has become accessible.

Reference source: https://www.wko.at/datenschutz/eu-dsgvo-oesterreichisches-datenschutzgesetz (For further specifics, see ibid.)

Your rights

The General Data Protection Regulation regulates your rights. The exercise of these rights is regulated in Art. 12 GDPR. If the controller has reasonable doubts about the identity of the natural person making a request for information, deletion, etc., the controller may request additional information necessary to confirm the identity of the natural person.

As a person concerned, you have the following rights under the GDPR and FADP (Federal act concerning the protection of personal data

(https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html):

Fundamental right to data protection (Art. 1 Para. 1 FADP)

You shall have the right to secrecy of the personal data concerning that person, insofar as that person has an interest which deserves such protection. This means that your data must always be treated confidentially and may not be made accessible to others. The fundamental right to data protection in Art. 1 Para. 1 FADP also exists when the GDPR applies.

Right of access by the data subject (Art. 15 GDPR)

You have the right to know whether data about you is being processed by us. To exercise this right, you must submit a request to the controller. The data protection Authority offers a non-binding form for this purpose: (https://www.dsb.gv.at/download-links/dokumente.html). The controller must provide the information in a commonly used electronic format, unless otherwise specified in the request for information. The right to information does not exist if a business or trade secrets of us or third parties would be endangered by the provision of this information. The term " controller" here refers to all companies or individuals that receive, store or process personal data. For the purposes of this Privacy statement, these are: Zotter Alexander (email: contact@alexander-zotter.at), 1&1 Ionos and Microsoft Inc.

Right to rectification (Art. 16 GDPR)

You have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning you. It is also possible to request the completion of an incomplete data set by means of a supplementary declaration. You have the right to obtain from the controller restriction of processing, until the accuracy of the data can be determined (Art. 18 Para. 1 GDPR). To exercise this right, you must submit a request to the controller. The data protection Authority offers a non-binding form for this purpose: (https://www.dsb.gv.at/download-links/dokumente.html).

Right to erasure and withdrawal of consent (Art. 17 GDPR)

You have the right to obtain from the controller the erasure of personal data concerning you, where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- you withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- You objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or you objects to the processing pursuant to Article 21(2);
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject

There are restrictions on the right to erasure, e.g. if the data is used to defend legal claims (Art. 17 Para. 3 GDPR). If you consider the processing to be unlawful but oppose the erasure, you can request a restriction of processing in accordance with Art. 18 GDPR. To exercise this right, you must submit a request to the controller. The data protection Authority offers a non-binding form for this purpose: (https://www.dsb.gv.at/download-links/dokumente.html).

Right to restriction of processing (Art. 18 GDPR)

Art. 18 GDPR has the purpose of restricting the use of data without deleting it. The restriction of processing may be demanded in parallel with the right to rectification and the right to withdrawal of consent. If you consider the processing to be unlawful but oppose the erasure, you can request a restriction of processing. (Art. 18 Para. 1 S. b GDPR). To exercise this right, you must submit a request to the controller. The data protection Authority offers a non-binding form for this purpose: (https://www.dsb.gv.at/download-links/dokumente.html).

Right to data portability (Art. 20 GDPR)

The right to data portability grants the right to receive data in a structured, commonly used and machine-readable format and to give this data to another controller for processing. The right to data portability differs from the right to information in that the emphasis is on portability. This right only exists if the processing is based on consent and the processing is carried out by automated means. To exercise this right, you must submit a request to the controller. The data protection Authority offers a non-binding form for this purpose: (https://www.dsb.gv.at/download-links/dokumente.html).

Right to object (Art. 21 GDPR)

Sie haben das Recht, jederzeit gegen die Verarbeitung Ihrer personenbezogenen Daten, die aufgrund von Art. 6 Absatz 1 lit. f GDPR (siehe Abschnitt Rechtsgrundlagen) erfolgt, Widerspruch einzulegen. You have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning you which is based on points (e) or (f) of Article 6(1). To exercise this right, you must submit a request to the controller. The data protection Authority offers a non-binding form for this purpose: (https://www.dsb.gv.at/download-links/dokumente.html).

Other rights

Right to lodge a complaint with a supervisory authority. In accordance with Art. 77 GDPR, you have the *right to lodge a complaint with a supervisory authority* if you believe that the processing of personal data concerning you violates the General Data Protection Regulation. Therefore, a complaint for violations of other provisions of the GDPR is also possible. The Data Protection Authority offers a non-binding form for this purpose: https://www.dsb.gv.at/download-links/dokumente.html.

Source of the text passages above: https://www.dsb.gv.at/aufgaben-taetigkeiten/rechte-der-betroffenen.html

Data Types

Informational use of our website

When using our website for informational purposes only, we collect data in a server log file. For the data created in it, see the "Server Log File" section. This and other personal data will be collected for the duration of the session and will not be stored or shared by us moreover that. The purpose of data collection is to establish a connection, to ensure the smooth use of the website, to optimise the website and to evaluate system security and stability. (Legal basis: Legitimate interests Art. 6 Para. 1 S. f GDPR)

Contact via contact form/support ticket/email/post etc.

If you contact us via a form on the website, email, post, etc., the following data will be collected: Reason for the request, first name and last name, email, your message, creation date of the request, and processing status of the request.

If you have a user account and are logged in, you can also communicate with us via chat. When you communicate in a chat, the following data is transmitted and stored: user, creation date, chat history. For the purpose of processing the enquiry and in the event of follow-up questions, this data will be stored for six months. The storage takes place on our server at 1&1 IONOS (see section "1&1 IONOS").

(Legal basis: pre-contractual measures and order processing or legitimate interests Art. 6 para. 1 s. b and f GDPR). We do not pass on this data without your consent.

The data can be used for processing and storage for the following tasks:

- to respond to enquiries
- for preparation and conclusion of a contract.
- for preservation of evidence for liability reasons
- for the fulfilment of statutory record retention of business letters (https://www.wko.at/datenschutz/eu-dsgvo-speicher-und-aufbewahrungsfristen)

(Legal basis: Art. 6, Para. 1. S. b and f GDPR)

Support Tickets

Support tickets are used to answer user questions and troubleshoot problems for users. You can only create support tickets if you have an active user account. When a support ticket is created, it is stored in the user account. The data collected during the creation of the support ticket (subject, message, creation date), as well as the whole communication traffic will be stored (and remain available to you) and will be deleted after the account has been deleted.

The data can be used for processing and storage for the following tasks:

- to respond to enquiries
- to resolve problems that occur when using our website.
- for preservation of evidence for liability reasons

(Legal basis: Art. 6, Para. 1. S. b and f GDPR)

Registration, Login, User Account, Affiliate Program

Users can create a user account on our website. As part of the registration process, the necessary information is recorded and stored.

The following data is collected, stored and processed: Username, first name, last name, password as well as an email address, registration date, permissions, account status (active / inactive) If the account is deleted, it will first be deactivated for 14 days and then deleted. (Legal basis: Art. 6, Para. 1. S. b and f GDPR) As with every visit to a website, a server log file is created (see section "Server log file"). The aforementioned data will not be passed on to third parties, unless this is necessary to pursue our claims or there is a legal obligation to do so. The data will only be passed on to third parties with the user's consent. User accounts are not public and cannot be recorded by search engines. (Legal basis: Art. 6, Para. 1. S. a, c, f GDPR)

If you have a user account, you can also log in via your Microsoft account, Discord account or Google account.

For the transfer of funds within the framework of our affiliate program, your account data (IBAN, BIC, account holder) will be stored.

Microsoft:

When you log in to our website via your Microsoft account, the following data is transmitted to us and stored: display name, first/last name, email, job title, business phone number, phone number, preferred language, Microsoft ID. This data is stored either until your account is closed or until your Microsoft account is unlinked. We do not transfer any personal data to Microsoft or third parties in this context.

Discord:

When you log in to our website via your Discord account, the following data is transmitted to us and stored: Discord ID, username, avatar URL, global name, email, verification status. This data is stored either until your account is closed or until your Discord account is unlinked. We do not transfer any personal data to Discord or third parties in this context.

Google:

When you log in to our website via your Google account, the following data is transmitted to us and stored: Google ID, display name, first/last name, email, verification status. This data is stored either until your account is closed or until your Google account is unlinked. We do not transfer any personal data to Google or third parties in this context.

Storage time of data

Your data will be deleted if:

- the purpose of processing of the data is no longer applicable

- The consent has been withdrawn, which is a prerequisite for processing
- they are no longer necessary for the exercise or defence of legal claims or for the protection of the rights of another natural or legal person,

If you have an active account, we will store your data for two years after your last access to the account. This privacy statement contains further information on storage/deletion of data, that takes precedence over determinations above.

Profiling and direct marketing

We do not use profiling and you will not receive direct marketing from us.

Cookies

Our website uses a session cookie. These are small text files that are stored on your device with help of your browser. They do not contain any personal data. They do not cause any harm. We use cookies exclusively for technical reasons in order to be able to offer our information and services in a functional manner. The session cookie is set as soon as you log in to our website. The cookie is set to maintain your login status. You will remain logged in until the session cookie expires or you actively log out. When you log out, the cookie is deleted. If you disable cookies, the functionality of our website may be limited. If you do not log in to our website, we will not set cookies.

Server-Logfiles

When you access our online offer (website), a "server logfile" is created at 1&1 IONOS. Server log files are created as soon as you open our website. To this, you do not need to register or log in. Log files make it easier to avert the danger of cyber attacks (e.g. DDoS attacks) and increase stability of servers. (Legal basis: Art. 6, Para. 1. S. f GDPR)

The following data about you is stored in the server log file: your IP address (due to privacy policies on personal data, the IP addresses of the callers are anonymized in the log files.); referrer URL (the previously visited page); address and name of the websites and files accessed; time/date of call; notification of successful call, browser type (and version), operating system and device type, amount of data transferred, your provider.

The processing of the data provided is not required by law or contract. However, the functionality of the website is not guaranteed without the processing. The server logfile data will not be passed on to third parties or transferred to a country outside the EU. Server log file data is stored for a period of 30 days and then deleted or anonymized. If required by law, the data will be exempted from deletion until the incident has been clarified.

Data transfer

As part of our processing of personal data, we use the services of third parties (web hosting, display of fonts and icons, etc.). We always comply with the legal requirements and only conclude contracts with third-party providers who guarantee protection of your data.

Data traffic within the EU (as well as Liechtenstein, Iceland and Norway) is not subject to any restrictions due to the same level of data protection guaranteed by the GDPR.

If we process your data in a third country (i.e. outside the European Union) or if the processing takes place in the context of the use of third-party services, this will only take place in accordance with the legal requirements.

Data traffic with third countries is only permitted under the following conditions:

1. Existing Commission adequacy decision

Data transfers on the basis of an adequacy decision (Art. 45 GDPR) do not require special approval by the supervisory authority. You can view EU adequacy decisions here: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en?prefLang=de.

Particular case USA:

Personal data may only be transferred to those US companies based on the DPF (EU-US Trans-Atlantic Data Privacy Framework) that have been registered in the "Data Privacy Framework List" at the US Department of Commerce in advance after certification. These certified U.S. companies commit to complying with a number of detailed data protection obligations, such as appropriation, data minimization, retention period, and data security. The list of certified companies can be found here: https://www.dataprivacyframework.gov/.

2. Existence of appropriate guarantees

Ohne Genehmigung der Aufsichtsbehörde können diese geeigneten Garantien bestehen, in:

- standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2); .(Art. 46 Para. 2 S. c GDPR)
- binding corporate rules in accordance with Article 47;
- an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Exceptions for certain cases (without approval from the supervisory authority)

- You have given your explicit consent.
- The transfer is necessary for the assertion, exercise or defence of legal claims.
- The data transfer is required by law (Art. 49 Para. 1 GDPR).

Source: https://www.wko.at/datenschutz/eu-dsgvo-internationaler-datenverkehr
In this privacy statement, we inform you for each service provider which requirements are met for a data transfer.

Security Data Transfer

TLS/SSL encryption

We use TLS/SSL encryption to protect your data transmitted through our online services. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are the most widely used security protocols on Internet. If your computer, smartphone or tablet connects to a secure website, the SSL protocol ensures a risk-free and encrypted end-to-end connection. TLS/SSL prevents hackers from reading or stealing the transmitted information. You can recognize this encryption by a "https://" in the URL or by a security lock that is displayed in the address bar of your browser.
Source: https://www.wko.at/vlbg/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/was-ist-ssl

Transfer of data

We share your data with application providers that you authorize. You can authorize providers, as long as they have integrated "to do". To do this, you must grant access permissions to the provider.

You can grant the following access permissions to providers:

- Username, first name, last name, email (stored in "to do").
  [Access to this data is mandatory and cannot be denied.]
- The application has access to information from your linked Discord account. This includes username, region, email, and Discord ID.
- The application has access to information about your linked Microsoft account. This includes username, first and last name, email, and Microsoft ID.
- The application has access to information from your linked Google account. This includes username, first and last name, email and Google-ID.

As part of the processing, it may also be necessary to transfer your data to third parties: insurance companies, courts, authorities (including tax offices), lawyers, tax consultants, auditors. Your data will be transfered on the basis of legal regulations or because our interests in processing the data outweigh the interests. (Art. 6, para. 1 lit. b and f. GDPR).).

Providers and services used

Webhosting

1&1 IONOS

For the publication of our website, we use the web hosting of the company 1&1 IONOS, with which we have concluded an AV contract. Web hosting means provision of storage space (web space) for publishing websites. If you want to publish a website on the Internet, you have to use web hosting. For a more detailed description of how web hosting works, see:
https://www.ionos.at/digitalguide/hosting/hosting-technik/was-ist-webhosting/

We use the web hosting of 1&1 IONOS to provide a secure and fast online offer. We use storage space on the web to host our website, store data and transmit data. We do not use any other services from 1&1 IONOS. 1&1 IONOS does not collect any personal data on our behalf. Our email correspondence also takes place via 1&1 IONOS. IONOS does not access the content of your emails.

1&1 IONOS

Office:

Germany: 1&1 IONOS SE, Elgendorfer Str. 57, 56410 Montabaur

Austria: Mail Boxes Etc. AT0051; IONOS SE, Gumpendorfer Straße 142/PF 266, 1060 Wien

Legal basis: Legitimate interests (Art. 6 Para. 1 S f GDPR)
Website: https://www.ionos.at/
Privacy Statement: https://www.ionos.de/terms-gtc/datenschutzerklaerung/?linkId=ft.nav.privacypolicy
Transfer to third countries: not to apply, because the data transfer with 1&1 IONOS SE takes place within the EU

Microsoft Azure

We use the cloud and cloud software services Microsoft Azure offered by Microsoft Inc. to store, manage and exchange documents, content and information with users. In general, all Microsoft Cloud services we use are operated in the EU data centers in the European geographic region. Also, processing of personal data takes place in data centers of the geographical region of Europe. Data center locations in the Europe region are, for example: Austria, Finland, Ireland, Netherlands. For information about where Microsoft stores customer data, see: https://learn.microsoft.com/de-de/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide. This may also require a transfer of personal data to a country outside the European Union – specifically to the USA.
On communication processes, server log files are created by Microsoft (for data storage of log files, see section "Web hosting/server log file"). Microsoft itself processes user and metadata, which is used by Microsoft for security reasons and for service optimization. In context of the use of publicly accessible documents, websites or other content, Microsoft may store cookies on the user's computer for the purposes of web analysis or to remember user settings. (for use and restriction options, see: https://privacy.microsoft.com/de-de/privacystatement) Microsoft doesn't access your data stored in the cloud.

Microsoft, Inc

Office:

One Microsoft Place, South County Business Park, Leopardstown Dublin 18, Ireland

Headquarter: One Microsoft Way Redmond, Washington 98052, USA

Legal basis: Legitimate interests (Art. 6 Para. 1 S. f GDPR)
Website: https://www.microsoft.com/de-at
Privacy statement: https://privacy.microsoft.com/de-de/privacystatement
Third country transfer: active in the EU-US Data Privacy Framework List

(https://www.dataprivacyframework.gov/list)
Furthermore, the processing of data in the United States of America is legally covered by the standard contractual clauses of the European Commission, which are part of the contract with Microsoft Corporation (Art. 46 para. 2 S c GDPR).

Stripe

As part of contractual relationships, we offer you the payment services of the payment service provider Stripe, as a secure and efficient payment option. Payment services are provided within the EU by Stripe Payments Europe, Limited (SPEL), 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Ireland.
In order to process payment transactions, we transfer the necessary payment data to Stripe Payments Europe Ltd.: data for the creation of the invoice (product name, gross price, currency, VAT rate, etc.), time when the payment button was pressed, your e-mail address.
Stripe requests and processes personal data: name, address data, email address, credit card details, promotion codes. This data is required for the processing of payment transactions, but also to defend against fraud attempts and for financial reporting. The data is stored by Stripe for this purpose. The payment itself is processed entirely by Stripe. Stripe's terms and conditions and privacy statement apply. If necessary, Stripe Payments Europe Ltd. will also transmit the data to Stripe, Inc. in the USA.

Data will be deleted by Stripe as soon as the purpose for which it was stored no longer applies. Exceptions to this exist if further storage is necessary for evidentiary purposes or if there are legal obligation to preserve records to the contrary. When these storage reasons expire, the data will be deleted.

„Stripe and its service providers use and store personal data including cardholder PANs, contact information, and transaction history to authenticate cardholders using one time passcodes and knowledge of past transactions. These measures help combat fraud by increasing the likelihood that the person offering a card for payment is an authorized user.“ (See also: https://stripe.com/at/legal/privacy-center#what-data-may-be-shared-or-made-available-to-enable-me-to-see-stripe-ads-on-other-sites; https://stripe.com/de/legal/privacy-center#data-transfers)
Stripe does not sell personal information to third parties. Data is shared with a limited number of Stripe partners and to comply with legal requirements (e.g., as part of financial obligations). „In addition to Stripe’s sub-processors, we may also share Business Users’ onboarding data and payment instrument information with third party business partners when this is necessary to provide our services to our Business Users. We do so, for example, for the purposes of offering payment processing services to our Business Users or facilitating payment settlements.
Third parties to whom we may disclose personal data for this purpose are banks, payment method providers and payment processors, including, but not limited to“ (e.g. Mastercard Europe S.A.) See also: https://stripe.com/at/legal/privacy-center

We also receive data from Stripe: The invoice created, with the invoice data. This will be stored in accordance with the statutory retention obligations and then deleted; Data about the payment status. We do not receive any information regarding your account or credit card.

Stripe uses cookies to

- ensure that Stripe services run properly,
- detect and prevent fraud,
- understand how visitors use and interact with Stripe's website, and
- analyze and improve Stripe´s services.

See in detail: https://stripe.com/de/legal/cookies-policy

You have the right to information, the right to rectification and deletion of your data vis-à-vis Stripe, provided that there are no legal obligations to the contrary. If you have any questions, you can contact Stripe directly: https://support.stripe.com/contact/email

Stripe

Office:

Stripe Payments Europe, Limited (SPEL), 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Ireland

Headquarter: Stripe, Inc., 510 Townsend Street, San Francisco, CA 94103, USA

Legal basis: Vertragserfüllung und vorvertragliche Maßnahmen (Art. 6 Abs. 1 S. 1 lit. b DSGVO)

Website: https://stripe.com/

Privacy statement: https://stripe.com/de/privacy/

Third country transfer: active in the EU-US Data Privacy Framework List (https://www.dataprivacyframework.gov/list)

As at: **21. January 2025**