

Privacy Policy

At OneLog, your privacy is respected and protected. We strive for the highest level of data security, and our data protection regulations give you an overview of which personal data is collected, processed and passed on when you use our free registration and log-in service.

It is important that you read and understand our privacy policy.

Contents

1.	What is OneLog?	3
2.	Who is behind OneLog?	3
3.	Who is responsible for data processing?	3
4.	How can you contact us?	3
5.	What data is processed when you use OneLog?	4
5.1	What is personal data and what does 'processing' mean?	4
5.1.1	How and on what legal basis do we process your personal data?	4
5.1.2	What personal data is processed when you use OneLog and for what purpose?	5
a)	OneLog registration	
b)	Statistics and analyses relating to the use of digital services	
5.1.3	Other OneLog registration and login options	6
a)	Registration/login with SwissID	
b)	Registration/login via Facebook (social sign-in)	
c)	Registration/login via Google (social sign-in)	
d)	Registration/login with Apple (social sign-in)	
e)	Login with WebAuthn	
5.2	What non-personal data is processed when you use OneLog?	7
6.	What technologies do we use and how do we use them?	8
6.1	Cookies	8
6.2	We use the following Google services at OneLog to analyse your surfing behaviour:	9
6.2.1	Google Analytics	9
6.2.2	Google Tag Manager	10
6.2.3	reCaptcha	10
6.3	Sentry	11
6.4	Log files	11
7.	How and when is your data shared?	11
8.	Is your data transmitted abroad?	12
9.	How is your data secured?	12
10.	How long is your data stored for?	13
11.	What are my rights when it comes to personal data?	13
11.1	Right of access	13
11.2	Right to have your personal data rectified	13
11.3	Right to have your personal data erased	14
11.4	Right to have the processing of your personal data restricted	14
11.5	Right to data portability	14
11.6	Right to object	14
11.7	Withdrawal of consent	14
11.8	Right to lodge a complaint	14
12.	Changes to this privacy policy	15

Dear customer,

This privacy policy gives you an overview of the personal data concerning you that we (hereinafter referred to as '**OneLog**' or '**us**') collect, process and share when you use the free registration and login service. You will also learn about the rights you have regarding data protection and how you can exercise these.

Please note that all companies that have implemented OneLog (hereinafter referred to as '**affiliated companies**') have their own privacy policies which contain details on how each company processes personal data. The use of websites and mobile applications (hereinafter referred to as '**digital services**') from companies that use OneLog are therefore subject to the company-specific privacy policies in addition to this privacy policy. These are referred to when you use the digital services offered by the company for the first time. If there are any discrepancies between this privacy policy and the company-specific privacy policy, the latter shall take precedence.

Please read this privacy policy at regular intervals so that you are always up-to-date on what happens to your personal data when you use OneLog and so that you can exercise your rights.

1. What is OneLog?

OneLog allows you to log in to all digital services for which OneLog has been implemented following one-time registration and authentication via OneLog, without the need for a further authentication process.

2. Who is behind OneLog?

OneLog is a joint venture of Ringier AG, TX Group AG, NZZ AG and CH Media. The OneLog joint venture was set up to develop and operate a joint single sign-on solution for the Swiss Digital Alliance.

3. Who is responsible for data processing?

The controller is OneLog AG, c/o Ringier AG, Dufourstrasse 23, 8008 Zurich.

If the General Data Protection Regulation (EU GDPR) applies to data processing carried out by us, our EU representative is:

DSM Avocat à la Cour
Renaud LE SQUEREN
L-2146 Luxembourg
B.P. 2648 | L-1026 Luxembourg
eu-representative-onelog@dsm.legal

4. How can you contact us?

You have different options when it comes to contacting us:

If you have a question regarding **data protection law**, you can send an **email or letter** to OneLog's data protection advisor:

Email address

datenschutz@onelog.ch

Postal address

OneLog AG
c/o Ringier AG
Data protection
Dufourstrasse 23
8008 Zurich

If you have a **question** regarding your **OneLog account**, you can send us an email or contact us via our contact form:

Email address

support@onelog.ch

Contact form

<https://onelog.ch/support>

When using the contact form, please enter your first name, last name, email address and message so that we are able to process your request. Your information is provided on a voluntary basis.

5. What data is processed when you use OneLog?

There are essentially two categories of data that are processed when you use OneLog: **personal data** (section 5.1) and **non-personal data** (section 5.2).

5.1 What is personal data and what does 'processing' mean?

Personal data is any information that concerns you and reveals something about you. As an example, this could be your first name, last name, postal address, email address, date of birth, telephone number or similar information.

Information that cannot be linked to you personally, i.e. your identity, is not considered to be personal data. It is anonymous.

Processing refers to any handling of your personal data. Among other things, this refers to the recording, collection, anonymisation, storage, administration, use, transmission, disclosure and erasure of your personal data.

5.1.1 How and on what legal basis do we process your personal data?

Your trust in us protecting your personal data and therefore you as a person is important to us. That's why we want you to know the following:

We adhere to the principles imposed by Switzerland's data protection laws and those of the European Union, if applicable. This means that we transparently explain to you the type of personal data we process and for what purpose. We only process personal data that we have obtained lawfully and for which we have a legal basis for processing, if needed. A legal basis can be a contract, your consent, a law or a public interest that allows us to process it or a legitimate interest on our part.

Whenever we process your personal data, we will inform you of what we intend to do with it. If we no longer need your personal data and are no longer legally obliged to store it or you no longer want us to store and process it, then we will stop doing so.

You can find out what rights you have with respect to your personal data and how you can exercise them in section 11 below.

5.1.2 What personal data is processed when you use OneLog and for what purpose?

If you use OneLog, we and any affiliated companies process your personal data for the following purposes:

a) OneLog registration

When you register with OneLog, you will receive a cross-platform user account (hereinafter referred to as the '**OneLog account**'). Collection of the following personal data is required from you on registration:

- Email address
- Salutation (optional)
- First name (optional)
- Last name (optional)

This personal data is processed for the following purposes:

- to fulfil the user contract between you and OneLog;
- to create a OneLog account;
- to check access authorisations and to administer and manage the OneLog account; and
- to provide OneLog and digital services offered by affiliated companies.

Please note that some affiliated companies collect and process additional personal data to allow them to provide their digital services to you. A more detailed description can be found in each company's privacy policy.

b) Statistics and analyses relating to the use of digital services

We compile statistics and analyses to allow us to better analyse and evaluate how our digital services are used.

5.1.3 Other OneLog registration and login options

a) Registration/login with SwissID

You have the option of registering with or logging in to OneLog using SwissID – a Switzerland-wide uniform login from SwissSign Group AG (hereinafter referred to as '**SwissSign**'). If you do this, we receive the personal data required by SwissSign Group AG for registration or login (salutation, first name, last name, email address).

OneLog has no control over the scope of data collected by SwissSign if you use SwissID. You can find more information about the purpose and scope of collection as well as the further processing and use of your data by SwissSign Group AG, your rights and settings options to protect your data in SwissSign Group AG's privacy policy: [Data protection | SwissID](#).

Please note that some affiliated companies request and process additional personal data to allow them to provide their digital services to you. A more detailed description can be found in each company's privacy policy.

b) Registration/login via Facebook (social sign-in)

You have the option of registering with or logging in to OneLog using your Facebook account. If you do this, we receive the personal data required by Facebook for registration or login (salutation [optional], first name, last name, email address).

OneLog has no control over how Facebook handles data collected via Facebook login. You can find more information about the purpose and scope of collection as well as the further processing and use of your data by Facebook, your rights and settings options to protect your data in Facebook's privacy policy: [Facebook](#).

Please note that some affiliated companies request and process additional personal data to allow them to provide their digital services to you. A more detailed description can be found in each company's privacy policy.

c) Registration/login via Google (social sign-in)

You have the option of registering with or logging in to OneLog using your Google account. If you do this, we receive the personal data required by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland (hereinafter referred to as '**Google**') for registration or login (salutation [optional], first name, last name, email address).

OneLog has no control over how Google handles data collected via Google login. You can find more information about the purpose and scope of collection as well as the further processing and use of your data by Google, your rights and settings options to protect your data in Google's privacy policy: [Privacy policy – Privacy policy & terms of use – Google](#).

Please note that some affiliated companies request and process additional personal data to allow them to provide their digital services to you. A more detailed description can be found in each company's privacy policy.

d) Registration/login with Apple (social sign-in)

You have the option of registering with or logging in to OneLog using your Apple account. If you do this, we receive the data required by Apple Inc. One Apple Park Way, Cupertino, CA, 95014, USA for registration or login.

OneLog has no control over how Apple handles data collected via Sign in with Apple. You can find more information about the purpose and scope of collection as well as the further processing and use of your data by Apple, your rights and settings options to protect your data in Apple's privacy policy: [Apple privacy policy - Apple](#).

Please note that some affiliated companies request and process additional personal data to allow them to provide their digital services to you. A more detailed description can be found in each company's privacy policy.

e) Login with WebAuthn

You have the option of logging in to OneLog on a voluntary basis using various forms of WebAuthn (e.g. Apple Touch ID and Face ID).

In these cases, OneLog does not receive any personal data from the provider. Your device is identified using encrypted and anonymised data. You can find more information on this from the software or hardware providers in question – via the following link for Apple, for example: [Data protection - Control - Apple \(CH\)](#).

5.2 What non-personal data is processed when you use OneLog?

Non-personal data is information that cannot be linked to you personally, i.e. your identity. As such, this data is anonymous for us.

We collect and process this data so that we can continuously improve OneLog and adapt it to your needs, identify trends, and compile and evaluate statistics on how OneLog is used.

6. What technologies do we use and how do we use them?

We use the following technologies:

6.1 Cookies

Cookies can be split into session cookies and persistent cookies.

- Session cookies can be used to track the websites you have visited and the options you have used. A session cookie is only saved for the duration of your online visit, i.e. during a single Internet session. The session ends and the cookie is deleted when you close your web browser.
- Among other things, persistent cookies can be used to recognise you again on a subsequent visit and to recognise your preferences such as your reading preferences, for example. A persistent cookie is stored for longer than a single session.

Cookies can also be split into functional and non-functional cookies. OneLog uses both functional and non-functional cookies on the OneLog website:

- Functional cookies are necessary to ensure the functionality of websites or services.
- Non-functional cookies are not absolutely necessary for website functionality. This type of cookie is used to collect and analyse data on website usage or the use of mobile applications (language preferences, duration of a session, etc.).

You can manage and/or delete cookies at any time by using the opt-out link provided above. Most web browsers automatically accept certain cookies by default. However, you are free to change your browser settings so that cookies are generally rejected by selecting 'do not accept cookies' in your browser settings, or by being asked first before your browser accepts a cookie from a website you visit. You also have the option of deleting cookies on your computer or mobile device by using the relevant browser feature. Please be aware that you must disable or delete cookies on all of your devices. Please note that by deleting cookies in your browser, you will also delete the opt-out cookie, i.e. if you still want to have an opt-out cookie enabled and have deleted all of the cookies, you must re-enable the opt out cookie when you visit this website again. Otherwise, you will be recognised as a new user and your data will be collected again. Please also be aware that you must disable cookies on all of your devices. If you choose one of these options, you may be unable to use all of the website's features to their full extent.

You can click on the following links to find out more about this option for the most commonly used browsers:

[Google Chrome](#)

[Microsoft Edge](#)

[Mozilla Firefox](#)

[Apple Safari](#)

6.2 We use the following Google services at OneLog to analyse your surfing behaviour:

6.2.1 Google Analytics

On our website, we use Google Universal Analytics and Google Analytics 4 (collectively referred to as “Google Analytics”), web analytics services provided by Google that enable an analysis of your use of our website.

Google Analytics uses cookies that are stored on your device (laptop, tablet, smart phone, etc.) and enable an analysis of your use of our website. This enables us to evaluate the usage behaviour on our website and to make our offer more interesting by means of the statistics/reports obtained.

For Google Analytics, the anonymisation of IP addresses is activated by default. This means that your IP address is shortened by Google within Switzerland or the EU/EEA before it is transmitted. Only in exceptional cases will the full IP address be transmitted to a Google server and shortened there.

We have concluded an order processing contract with Google, which ensures the protection of our site visitors’ data and prohibits unauthorised disclosure to third parties. For the transfer of data to the USA, Google refers to standard contractual clauses of the European Commission, which are intended to ensure compliance with the European level of data protection. Further legal information on Google Analytics, including a copy of the aforementioned standard contractual clauses, can be found [here](#).

As an extension to Google Analytics, the “UserIDs” function can be used on the website. If you log in on different devices with your account, your activities can be analysed across devices.

Google uses this information to evaluate your use of our websites, to compile reports on website activity and to provide us with other services related to website and internet use.

If you allow cookies to be stored, Google Analytics 4 will retain your data for two months. Data for which the end of this retention period has been reached will be automatically deleted.

An overview of the data use in Google Analytics and the measures taken by Google to protect your data can be found in the Google Analytics Help.

If you are outside Switzerland, all the data processing described, including data transmission by pings and the possible setting of Google Analytics cookies, will only take place if you have expressly consented to this via the cookie banner displayed. Without your consent, Google Analytics will not be used during your visit to the website. You can revoke your consent at any time with effect for the future. To exercise your right of revocation, please deactivate this service via the “Cookie Consent Tool” provided on the website.

You can prevent the collection and transmission of the data generated by the cookie and related to your use of our websites to Google, as well as the processing of this data by Google, by deactivating the cookies via the cookie setting.

You can find more information on the terms of use and data protection on the [download page for the browser add-on](#) to deactivate Google Analytics. You can also prevent cookies from being stored by setting your browser software accordingly.

6.2.2 Google Tag Manager

We also use Google Tag Manager to integrate Google analysis and marketing services into our website and to manage them. Google Tag Manager is a solution that you can use to manage website tags via an interface. The actual tool that implements tags is a cookie-free domain and does not collect any personal data. However, the tool enables other tags which may collect data. Google Tag Manager itself does not have access to this data. If tags have been disabled at domain or cookie level, this will remain in place for all tracking tags implemented using Google Tag Manager.

You can find more information about Google Tag Manager in the [Google Tag Manager Use Policy](#).

6.2.3 reCaptcha

We use reCaptcha on our website. ReCaptcha is an acronym for ‘completely automated public Turing test to tell computers and humans apart’. It is a test designed to distinguish people from machines/robot programs, or ‘bots’ for short. reCAPTCHA is a service that tries to determine whether a certain action on the internet is being carried out by a human being or by a computer program. reCAPTCHA is used as part of double opt-in when subscribing to the newsletter.

You can find more information about data processing and information on data protection by reCAPTCHA at: [Privacy policy – Privacy policy & terms of use – Google](#).

6.3 Sentry

We also use the service Sentry (Sentry, 1501 Mariposa St #408, San Francisco, CA 94107, USA) to improve the technical stability of our service by monitoring system stability and identifying code errors. Sentry serves these purposes alone and does not evaluate any data for advertising purposes. User data, such as information about the device or the time of the error, is collected anonymously and used in a non-personal way before being erased.

You can find more information about this in Sentry's privacy policy: [Application monitoring and error tracking software | Sentry](#).

6.4 Log files

When using OneLog, the web servers register usage data – known as log files. Log files provide information on your IP address, the operating system used, the pages you have visited, interactions on the pages, your browser version and settings, the date, and time. This information is technically necessary in order to correctly provide you with the website content requested, to ensure the system security and abuse prevention.

Such data is stored separately from any data you may have provided.

7. How and when is your data shared?

When you register with an affiliated company for a product for the first time, your personal data will be shared with that company and processed for the purposes mentioned above (section 5.1.2).

Your personal data may also be shared with third parties outside OneLog who provide technical or organisational services on behalf of OneLog where we need such services to fulfil the above-mentioned purposes or to carry out general business activities. We contractually oblige these service providers to process your personal data exclusively on our behalf as per our specifications and to ensure the protection of your personal data by implementing appropriate technical or organisational security measures.

We share your data with the following categories of recipients:

- affiliated companies;
- IT service providers;
- hosting partners;

- providers to which we have outsourced certain support services such as translation work or document reviews;
- third parties who provide services to us, such as law firms or other service consultancies.

Your personal data will not be passed on, transferred or sold to third parties outside OneLog unless this is necessary to process a contract that you have concluded with OneLog or you have given your explicit consent.

We may share personal data where this is required by law, for example if we are required to share personal data with a law enforcement agency or for the purpose of prosecuting or uncovering unlawful activities.

8. Is your data transmitted abroad?

If your personal data is also transmitted to third parties abroad, i.e. outside of Switzerland or the European Economic Area [EEA]), they are obliged to comply with data protection to the same extent as we are. If the specific country does not have an adequate level of data protection, we will ensure that your personal data does have an adequate level of data protection. In particular, we ensure this by concluding EU Commission 'standard data protection clauses' with the companies concerned and/or through binding corporate rules (BCR) for the companies concerned, recognised by a European data protection authority, and, if necessary, further guarantees. If this is not possible, we base the data transfer on your explicit consent or the necessity of the transmission to fulfil a contract.

9. How is your data secured?

OneLog operates secure data networks that meet all applicable technical standards. Appropriate technical and organisational measures are implemented to scrupulously protect your data from loss, destruction, falsification, manipulation and unauthorised access.

Although OneLog makes every effort to prevent the disclosure of data due to errors in data transmission and/or unauthorised access by third parties, it cannot accept any liability for such unwanted events.

10. How long is your data stored for?

We only process and store your personal data for the period necessary to achieve the purpose of storage or if this is required by laws or regulations to which we are subject. If the storage purpose no longer applies or if a set storage period expires, your data will be suppressed or erased by default and in line with any applicable legal provisions.

11. What are my rights when it comes to personal data?

You are entitled to determine what happens to your personal data yourself and you can always find out what happens to your personal data.

So that we are able to check your identity, we ask that you send the request directly from your OneLog account via email or, for written requests, to enclose a copy of proof of identity.

If you have a question regarding additional data collected by affiliated companies, please consult the company-specific privacy policy.

For questions in connection with data protection carried out by us and for information regarding your rights and how to assert them, you can contact us at any time using the contact options provided in section 4 of this privacy policy. If necessary, we reserve the right to request identification from you in a suitable manner in order to process requests.

You have the following rights under data protection law:

11.1 Right of access

You have the right to obtain from us confirmation as to whether or not and what personal data concerning you is being processed.

11.2 Right to have your personal data rectified

You have the right to obtain the rectification of inaccurate personal data concerning you and, where applicable, to have incomplete personal data concerning you completed in our systems.

11.3 Right to have your personal data erased

You have the right to request that your personal data is erased, e.g. if the data is no longer required for the intended purposes. However, if we are obliged to keep your personal data because of legal or contractual retention requirements, we are only able to restrict or suppress your personal data in these cases as far as this is necessary.

11.4 Right to have the processing of your personal data restricted

You have the right to ask us to restrict the processing of your personal data.

11.5 Right to data portability

You have the right to receive your personal data, which we process automatically on the basis of your consent or in order to fulfil a contract, in a structured, commonly used and machine-readable format or to request that such data is transmitted to a third party. If you ask us to directly transfer the data to another controller, this will only be done if this is technically feasible.

11.6 Right to object

You have the right to object to the processing of your personal data at any time, in accordance with legal provisions. In particular, you have the right to object to the processing of your personal data for the purpose of direct marketing.

11.7 Withdrawal of consent

If you have consented to the processing of your personal data, you are entitled to withdraw your consent at any time. If the processing of the personal data serves marketing and advertising purposes, you can withdraw your consent to processing for these purposes in general or in relation to specific products or services.

11.8 Right to lodge a complaint

You have the right to submit a report to the relevant supervisory authority or to lodge a complaint if you are of the opinion that the processing of your personal data is not in compliance with data protection regulations. You can do so with the supervisory authority in the country where you live or work, or in the town, city or country where the alleged data breach took place.

12.Changes to this privacy policy

OneLog adapts this privacy policy to new or changing needs. The new version will be made available to you in a suitable place.

The current privacy policy published by us applies in each case.

Version 2.6
September 2023