Yokoy Privacy Policy

Version 4.2 August 2023

1. Introduction

Data protection is of utmost importance to Yokoy. We ensure through various technical, organizational and contractual measures that your data is always kept up to date, stored securely and processed in accordance with Swiss (Federal Data Protection Act; RevFADP[1]) and European data protection regulations (in particular the General Data Protection Regulation GDPR[2]). This applies both in our company and in the cooperation with our partners and suppliers.

In addition, we have our software data security audited annually by independent external experts and implement their recommendations. Yokoy has also established an Information Security Management System (ISMS) in accordance with the requirements of the ISO 27001 standard, which was certified by TÜV Rheinland in November 2022.

With this privacy policy, we would like to inform you transparently about how we process your data.

A. Contact Yokoy
B. Personal data categories
C. What data we process
D. International data transmission
E. Data security
F. Data storage and deletion
G. Your rights
H. Privacy Policy Updates

2. Scope

This Privacy Policy applies to all entities of Yokoy. ("Yokoy" or "we"). The Cookie Policy applicable to all Yokoy entities is an integral part of this Privacy Policy. Our cookie policy can be found here: Yokoy Cookie Policy. You can also use our Cookiebot to granularly determine which optional cookies you want to allow and which you do not.

3. Responsibility and review

This privacy policy is reviewed at least once a year and signed off by our internal Data Protection Officer. The last update results from the versioning under the title.

[1] The reference to the FADP in this policy refers to the new FADP which enters into force on September 1st 2023.
[2] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data.

A. Contact Yokoy

Our Data Protection Officer is available to answer any questions you may have about data protection for all Yokoy entities.

1. Yokoy Headquarter

Yokoy Switzerland Ltd
MLaw Claudio Berther, LL.M (Law & Technology) University of California, Berkeley
Legal and Data Protection Officer
Förrlibuckstrasse 181
8005 Zurich
dpo@yokoy.ai
Tel. +41 (0)43 508 15 77
CHE-172.979.264

2. Yokoy Deutschland GmbH - Munich

Yokoy Deutschland GmbH
Unicorn Workspaces Isartor
Isartorplatz 8
80331 Munich
info@yokoy.ai
Tel: +49 151 42 04 31 22
Germany Commercial Register Number: HRB 267689

3. Yokoy GmbH Austria - Vienna

Yokoy GmbH.
Hamerlingplatz 8/17
1080 Vienna
info@yokoy.ai
Tel: +43 1 417 01 15
Managing Director: Mag. (FH) Stephan Hebenstreit, LL.M.
Commercial register court: Vienna Commercial Court
Number of the company register: FN 534254
UID: ATU75770818
Place of jurisdiction: Vienna Commercial Court
Chamber affiliation: Vienna Chamber of Commerce

Yokoy Netherlands B.V. - Amsterdam

Yokoy (Netherlands) B.V.
Singel 542
1017 AZ Amsterdam
KVK number 84480742
info@yokoy.ai
Tel. +31 6 20 33 28 90

B. Categories of personal data

The personal data as defined in Art. 5 RevFADP and Art. 4 GDPR we process are divided into the following categories

1. Basic data (e.g. last name, first name)
2. Contact details (e.g. telephone, email, postal address)
3. Browser and device data, meta or boundary data and usage data, content data that you submit to us (e.g., through the contact form, registration for newsletters, webinars, and protected content or applications).
4. Location data
5. Contact, sales, contract and payment data in our customer relationship management system
6. Uploaded receipts and eventually photographs thereof which may or may not contain personal data.

C. How we process data

1. Data you give us

You voluntarily provide us with data in various situations. For example, when you contact us, subscribe to our newsletter, register in the customer portal, apply for a job, register for a webinar or download protected content. If you want to know more about how we process this data, for what purpose and on what legal basis, read " C. 1. Data you give us or click here.

2. Data processed by us

In order to provide our services, maintain our infrastructure and provide the best possible experience to all stakeholders, we also process personal data. If you would like to know more about the purposes and legal basis for this, read "B. Data we process" or click here.

3. Data processed by our partners

To deliver our services, maintain our infrastructure, and provide the best possible experience for all stakeholders, we work with partners. They also process personal data. For example, when you visit our website, use the Yokoy app, or as part of our marketing and social media activities. If you would like to know more about the purpose and legal basis for this, please read "C. Data processed by our partners" or click here. In this context, we also refer you to our Cookie Policy, which can be found here: Yokoy Cookie Policy

D. International data transmission

Even though we strive to work with Swiss or European providers and make European data storage a condition when integrating new sub-processors wherever possible, the outflow of data abroad cannot be completely prevented. To find out how this is legally implemented by Yokoy in accordance with Art. 9 revFADP and Art. 28 GDPR and how your data is also transferred in a legally secure manner in connection with foreign transfers, please see "D. International Data Transfer" or click here. Yokoy will always keep an eye on this sensitive and constantly changing topic and adapt the international data transfer to the legal developments in this area.

E. Security of the data

The data disclosed to us is treated confidentially and protected against unauthorized access, damage or loss by technical and organizational measures according to Art. 8 revFADP and Art. 32 GDPR. To learn more about how we technically protect your data, see "F. Data Security" or click here. All Yokoy employees also sign a confidentiality agreement at the beginning of their employment. Our data security efforts comply with the internationally recognized ISO 27001 standard, to which Yokoy is externally certified by TÜV Rheinland. Furthermore, the security of our software is tested annually by an external third party through so-called penetration tests.

F Data storage and deletion

We store the data only as long as it is necessary for the fulfillment of the contract. This is subject to the statutory retention periods and your right to deletion in accordance with Art. 17 GDPR, provided that the requirements for this are met. If you want to know more about this topic, read F. data storage and data deletion" or click here.

G. Your rights

The RevFADP and the GDPR grants the person whose data is processed various rights with which the person can influence the data processing. For an overview of the rights and how you can exercise them, see G. Your rights or click here.

H. Privacy Policy Updates

We will inform you about adjustments and additions in an appropriate form, in particular by publishing the respective current privacy policy on our website. The processing of customer data is also regulated separately in a data processing agreement which forms part of the SaaS Agreement concluded with the customer.

A. Data you give us

1. Contact us

You can contact us through a variety of channels, including phone, email, contact form, chat, social media, webinar registration, and "gated content" registration. We collect your contact information and information from the inquiry. This information may be stored in our customer relationship management (CRM) system. This data is stored for internal use only.

1.1 Purpose of the processing

We store personal data in order to be able to respond to your inquiry or contact. Furthermore, this storage enables us to carry out the contract or pre-contractual measures in case of questions regarding an existing contractual relationship. In addition, Yokoy may conduct analyses about possible future contractual relationships, such as the size of the company, where the company is present and through which channels the company has heard about Yokoy.

1.2 Legal basis

The basis for the data processing is Art. 6 Para. 1 lit. b GDPR, which allows us to process data for the fulfillment of a contract or pre-contractual measures. The analysis purposes are based on the legal basis of legitimate interests according to Art. 6 Para. 1 lit. f GDPR to find out whether you fit into our customer portfolio in terms of size and geographical presence. The data processing is carried out in accordance with the data protection principles in Art. 6 RevFADP. We use the Hubspot and Salesforce software to enable this service. A link to their privacy policies can be found here HubSpot Privacy Policy Statement or here Salesforce Full Privacy Policy Statement.

2. Sign up for the newsletter

2.1 Purpose of the processing

Creation and sending of our newsletter.

2.2 Legal basis

If you subscribe to the newsletter, you give us permission to use your data for sending the newsletter. Furthermore, you agree to the information described below. Based on Art. 7 Para. 3 GDPR, you can revoke your consent at any time for the future; for this purpose, you will find an unsubscribe link in every email sent. We use the HubSpot software to send our newsletter. An overview of all partners with whom we cooperate for internal and external purposes, as well as links to their data protection declarations, can be found under " D. International data transfer" or click here.

2.3 Double opt-in procedure for the purpose of verifiability

An important principle of the General Data Protection Regulation is accountability. Art. 5 Para. 2 GDPR requires not only compliance with data protection regulations, but also proof thereof. For this reason, registration takes place in a double opt-in process. After your registration, you will receive an email in which you must confirm your email address. This prevents misuse with registrations from other email addresses. The registrations are stored in our CRM system so that we can legally prove the registration process. This includes the following data: Sign-up and confirmation time, type of newsletter, IP address and your contact details. The legal basis for this is the fulfillment of a legal obligation according to Art. 6 Para. 1 lit. c GDPR.

2.4 National specifications

Germany: The dispatch and performance measurement of the newsletter is based on the consent of the recipients in accordance with Art. 6 Para. 1 lit. a, Art. 7 GDPR in conjunction with. § Section 7 (2) No. 3 UWG or on the basis of the legal permission pursuant to Section 7 (3) UWG.
Austria: The dispatch of the newsletter and the associated performance measurement is based on the consent of the recipients pursuant to Art. 6 (1) a GDPR in conjunction with § 174 TKG. The logging of the registration process is based on our legitimate interests pursuant to Art. 6 Para. 1 lit. f GDPR. Our interest is directed towards the use of a user-friendly and secure newsletter software. In addition, there is a legal obligation to provide proof of registration. This obligation also results from accountability according to Art. 5 (3) GDPR.
Netherlands: Consent pursuant to Art. 6 (1) a GDPR in conjunction with Art. 11 (7) a Telecommunications Act.
Spain: Consent according to Art. 6 Para. 1 lit. a GDPR in connection with Art. 21 Para. 1 Law on Information Society and Electronic Commerce.
Switzerland: Data processing is carried out in accordance with the data protection principles pursuant to Art. 6 RevFADP.

3. Webinar registrations

You can also register for webinars via the Hubspot tool to get to know our products better. We store the data you provide so that we can contact you if necessary, e.g. if it becomes necessary to cancel the event. We base our data processing on your consent according to Art. 6 Para. 6 FADP and Art. 6 Para. 1 lit. a GDPR. This consent can also be revoked for the future in accordance with Art. 7 Para. 3 GDPR. To do so, contact us using the method described above in the Contact section. Data processing is carried out in accordance with the data protection principles pursuant to Art. 6 RevFADP.

4. gated content downloads

Gated content is about sharing knowledge that is valuable to the user in exchange for contact information of the user that is valuable to us. In the case of Yokoy, for example, this could be events on topics such as digitization, artificial intelligence, or data protection or automation.

4.1 Purpose of the processing

Content provision

4.2 Legal basis

We base our data processing on your consent pursuant to Art. 6 Para. 6 RevFADP and 6 Para. 1 lit. a GDPR. This consent can also be revoked for the future pursuant to Art. 7 Para. 3 GDPR. Contact us via one of the contact channels listed under contact above. Data processing is carried out in accordance with the data protection principles in Art. 6 RevFADP.

5. Applications

For job applications we use the service of Lever. Lever is GDPR and SOC 2 compliant. Employees and sub-processors are required to keep data strictly confidential. For more information, please visit the Lever privacy center. The applicant must also explicitly consent to the processing of their data via opt-in procedures and applicants can determine whether they wish to remain in the system in the event of an unsuccessful application in order to be contacted for newly advertised positions. In this case, the data will be deleted by system setting after two years at the latest. If the application is successful and a position is filled, the data is transferred to the Bamboo HR tool and retained until the duration of the contractual relationship. The data protection measures of BambooHR can be found in the Privacy Notice BambooHR.

5.1 Purpose of the processing

We process the personal data provided to us in order to review your application and to take pre-contractual measures and the conclusion of a possible employment contract with you. If your application is not successful or you withdraw your application and you do not wish to continue to be stored in our system, the data will be deleted within 30 days. If your application is successful, the data will be kept until the purpose is fulfilled, usually for the duration of the contractual relationship plus a period required by law.

5.2 Legal basis

The storage of the data is based on Art. 6 Para. 1 lit. b GDPR or the consent of the person according to Art. 6 Para. 1 lit. a GDPR. This consent can also be revoked for the future on the basis of Art. 7 Para. 3 GDPR. To do so, please contact the relevant contact person above. Data processing is carried out in accordance with the data protection principles pursuant to Art. 4 FADP.

B. Data processed by us

1. server log files

When you use our website, information that your browser transmits to us is automatically collected and stored. These are:

- Browser type and version
- The operating system
- IP address

- Referrer URL
- Host name of the computer
- Request date

We do not draw any conclusions about your person when using this data. Logging is done in accordance with our internal logging policy.

1.1 Purpose of the processing

The data is needed, for example, to deliver the content of our website correctly, to ensure the functionality of our website or to provide law enforcement authorities with the appropriate information in the event of a cyber attack. The anonymous data of the server log files are stored separately from your personal data.

1.2 Legal basis

We base the collection of this anonymized data on the legitimate interest of a functioning website according to Art. 6 Para. 1 lit. f GDPR.

2. Customer login/customer portal

The data protection provisions are agreed and signed with each customer when the contract is concluded (Data Processing Addendum as an appendix to the SaaS Agreement). The processing of customer data in our CRM system is carried out in accordance with point 3 below.
In addition, our system automatically records the following log data for each call:

- Browser type
- Amount of sent data in bytes
- Date and time of access
- IP address
- Language setting

2.1 Purpose of the processing

This data is collected for the purpose of providing the portal. In addition, this data is processed and stored to ensure the functionality of the portal and its security.

2.2 Legal basis

The data of the customer portal are processed according to Art. 6 Para. 1 lit. b and lit. f GDPR. The data is only stored as long as it is necessary for the fulfillment of the purpose. In order to provide the portal, data is also passed on to technically necessary partners, e.g. the website hoster Impsyde and the cloud provider Google Cloud Platform https://cloud.google.com/. An overview of all partners, their services, the legal basis for processing and contact options can be found under D. International data transfer. An internal logging and monitoring policy regulates the details.

3. Customer data (CRM Customer Relationship Management)

3.1 Purpose of processing

In order to provide our contractual services, we need to process data about our customers. In doing so, we process inventory data (e.g. customer master data, such as names or addresses), contact data (e.g. email, telephone numbers), content data (e.g. charts of accounts), contract data (e.g. subject matter of the contract, term), payment data (e.g. bank details, payment history). This mainly concerns customers, employees and suppliers. The purpose of the processing is the provision of contractual services, billing and customer service. For a more detailed description of the processing of customer data, please refer to the Data Processing Addendum. This forms part of our customer relationship as Annex 1, which is based on a SaaS (Software as a Service) contract.

3.2 Legal basis

The legal basis for the processing results from Art. 6 Para. 1 lit. b GDPR. We process data that is required for the establishment and performance of the contractual services. We process the data only for the contractual purpose and act in accordance with the legal requirements for commissioned processing pursuant to Art. 28 GDPR or 10a FADP. We delete the data after expiry of the contract or legal warranty and comparable obligations. In the case of legal archiving obligations, deletion takes place at the customer's request either at the end of the contract term or at the end of the legal retention periods, which vary depending on the country. Data processing is carried out in compliance with the data protection principles according to Art. 4 FADP. The data stored by us can be provided to the customer in .JSON or .csv format. For our CRM, we use the services of Salesforce. You can find out more about data protection under Salesforce Privacy Policy Here, the storage of data in the EU (Frankfurt / Dublin) is agreed with Salesforce.

C. Data collected from our partners

If we involve partners, this is done in accordance with the requirements of Art. 5 GDPR and Art. 5 lit. K and Art. 9 Para. 1 RevFADP. There are data processing contracts that meet the requirements of Art. 9 Para. 1 RevFADP and Art. 28 Para. 3 GDPR.

1. When visiting the website

In order to be able to operate a website technically, certain technical requirements are necessary, for which we rely on partners.

1.1 Hosting

1.1.1 Purpose of the processing

Our hosting provider Inpsyde provides us with infrastructure and platform services, database services, computing capacity, security services and storage space as well as technical maintenance services, which we use for the purpose of operating our online offering.

1.1.2 Legal basis

The basis for data processing is Art. 6 Para. 1 lit. b GDPR, which allows us to process data for the fulfillment of a contract or pre-contractual measures. Our website is hosted by Inpsyde GmbH, a German company that stores the data in Frankfurt. Privacy Inpsyde

1.2 Content Delivery Network (CDN)

1.2.1 Purpose of the processing

We use the open source services of js Delivr as a CDN to deliver the website quickly. js Delivr is a service of ProspectOne, Królewska 65A/1, 30-081, Krakow, Poland.
A CDN is a network of regionally distributed servers connected via the Internet. In order to use the service, it is possible that your browser sends personal data to jsDelivr. This may allow jsDelivr to collect and store data such as browser type/version, date and time of access or IP address. To avoid this, you can install a JavaScript blocker e.g. No Script

1.2.2 Legal basis

The basis for the use of the CDN is our legitimate interest in the optimization of the website according to Art. 6 Para. 1 lit. f GDPR. You can find more information here Privacy jsDelivr.

1.3 Google Web Fonts

1.3.1 Purpose of the processing

Our website uses so-called web fonts provided by Google to display fonts. The provider is Google Inc, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. This is a service of the American Google LLC. For users in the European Economic Area (EEA) and Switzerland, the Irish company Google Ireland Limited is responsible. When you call up a page, your browser loads the required web fonts into the browser cache in order to display texts and fonts correctly. For this purpose, the browser must establish a connection to Google's servers. In this way, Google learns that our website was accessed via your IP address.

1.3.2 Legal basis

The use of Google Web Fonts is in the interest of an appealing presentation of our website. This represents a legitimate interest within the meaning of Art. 6 Para. 1 lit. f GDPR. If your browser does not support web fonts, a standard font of your computer will be used. For more information, see Google Web Fonts FAQ and Google Privacy Policy: Google Privacy Policy.

1.4 YouTube

1.4.1 Purpose of the processing

To play the videos on our website, we use the services of YouTube. YouTube is a service of Google Inc. located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. When you visit one of our pages in which YouTube is embedded, a connection to the YouTube servers is created. This tells the YouTube server which of our pages you have visited. For more information on the handling of user data, please refer to YouTube's privacy policy. Privacy YouTube

1.4.2 Legal basis

The use of YouTube is based on Art. 6 Para. 1 lit. f GDPR. Information on how to prevent data collection can be found in the Yokoy Cookie Policy.

2. When you use the Yokoy app

The Yokoy App is hosted on Google Cloud Platform. Google Cloud Platform is a service provided by Google Ireland LLC, Google Building, Gordon House, Barrow St, Dublin 4, Ireland. Specific privacy information about Google Cloud can be found here: Privacy Google Cloud. Specific information about Google Cloud data security and our products can be found in the Data Security section or will be provided upon request.

Customers can download a mobile app to their device. The information required for this process is transmitted to the App Store without our intervention. The information includes, for example, the email address, the customer number of your App Store account or the time of the download. We are not responsible for this data collection and have no influence on it.
For more information, see Apple's or Google's privacy policies.
When using the Yokoy app, we process the following data to ensure the security and usability of the functions offered:

- Date and time of access
- IP address
- Access to the site
- The operating system
- Personal data as agreed in the privacy policy with the respective company. Name, first name, email and personnel number or cost center for publication.

In order to use the app in conjunction with the expense tool, the following categories are processed by the app: Last name, first name, email address and personnel or supplier number (for booking in the customer system) Further the uploaded expense documents or photographs thereof. For the invoice module, only the supplier's name and ID are required. Additional data can be provided by the user, but is not mandatory. For the Yokoy Pay module this is first name, last name, address, birthday and phone number. Detailed information is provided to our customers in the Data Processing Addendum, which is included in Appendix 1 and thus forms part of the contract concluded with Yokoy. A special addendum deals with the data processed within the framework of our Yokoy Pay module, as well as with the partners with whom we cooperate in order to realize this module.

The data is stored in an encrypted private cloud and the transfer to the Google Cloud is also secured with 256-bit AES encryption. By using the app, no employee data of the users is stored in our CRM.

2.1 Purpose of the data processing

This data is processed only for the provision of the Yokoy app.

2.2 Legal basis

This is done on the basis of Art. 6 Para. 1 lit. a, lit. b and lit. f GDPR.

3. Our marketing activities

3.1 Hubspot

On our website, we use the software HubSpot for various purposes. Our partner is Hubspot Deutschland GmbH, Am Postbahnhof 17, 10243 Berlin. Hubspot

3.1.1 Purpose of the processing

Hubspot uses web beacons and cookies to analyze your use of our website and to cover various aspects of online marketing. This includes email marketing, contact management (e.g. performance segmentation & CRM), landing pages and contact forms on our website and in the app. This information as well as parts of our website are stored on servers of our software partner HubSpot. It is used by us to contact visitors to our website and determine which of our company's services are of interest to them. The information collected is subject to this privacy policy. We use all collected information exclusively to optimize our marketing measures and to communicate with users.
As part of the optimization of our marketing measures, the following data, among others, may be collected and processed via HubSpot:

- Geographical location
- Browser
- The operating system
- IP address
- Duration of the visit
- Reference URL
- Information about how often the website is visited
- Newsletter subscription data
- Pages called

We also use HubSpot to provide contact forms on our website and on our app.

3.1.2 Legal basis

The legal basis for the processing is your consent pursuant to Art. 6 Para. 6 RevFADP and Art. 6 Para. 1 lit. a GDPR and for the necessary processing of personal data for the performance of a contract with the data subject as well as

for the implementation of pre-contractual measures pursuant to Art. 6 Para. 1 lit. b GDPR. If you do not want the aforementioned data to be collected and processed via Hubspot, you may refuse or revoke your consent at any time with effect for the future based on Art. 7 III GDPR. The personal data will be kept for as long as necessary for the purpose of the processing. The data will be deleted as soon as they are no longer required to fulfill the purpose. Here you can find more information about HubSpot's privacy policy.

3.2 Intercom

The chat function on our website and the Yokoy Academy at help.yokoy.ai are provided by Intercom. 2nd Floor, Stephen Court, 18-21 Saint Stephen's Green, Dublin 2. The data is stored in Dublin, Ireland.

3.2.1 Purpose of the processing

Chat function on our website and Yokoy Academy at help.yokoy.ai. User data analytics for the purpose of product development and direct-user communication about product updates. The analytics function can be disabled upon request.

3.2.2 Legal basis for processing

The chat function is a quick and convenient way for our customers to contact us as well the Yokoy Academy in support of our Yokoy customer service. These are legitimate interests according to Art. 6 I lit. f GDPR. You can find more information about Intercom's privacy policy here. Privacy Policy Intercom.

3.3 Google Tag Manager

3.3.1 Purpose of the processing

Our website uses the Google Tag Manager. The provider is Google Inc, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. Google Tag Manager is a solution that allows website tags to be managed via an interface. The Tag Manager tool (which implements the tags) is a cookieless domain and does not collect any personal data. The tool takes care of forwarding data and triggering other tags, which in turn may collect data. Google Tag Manager does not have access to this data. If a deactivation has been made at the domain or cookie level, it will remain in place for all tracking tags implemented with Google Tag Manager.

3.3.2 Legal basis

The legal basis for the use of Google Tag Manager is your consent pursuant to Art. 6 Para. 6 RevFADP Art. 6 Para. 1 lit. a GDPR. This can be revoked at any time based on Art. 7 (3) GDPR with effect for the future. To do so, please contact Yokoy.

3.3 Google reCaptcha

3.3.1 Purpose of the processing

The purpose of reCAPTCHA is to verify whether the data entry on our website (e.g. in a contact form) is made by a human or an automated program. The reCAPTCHA analyzes run entirely in the background. Visitors to the website are not notified that an analysis is being performed.

3.3.2 Legal basis

The data processing is based on Art. 6 Para. 1 lit. f GDPR. The website operator has a legitimate interest in protecting its web offers from abusive automated spying and from SPAM. For more information about Google reCAPTCHA and Google's privacy policy, please see the following links: Privacy Policy and Google reCAPTCHA V3.

3.3.3 Marketing tools that use cookies

Certain marketing tools use cookies. To learn what cookies are, what they do, and how you can disable them, visit our Cookie Policy or the Cookie Manager on our website. This allows you to fine-tune your consent to the use of cookies that are not strictly necessary to provide the website. You can find the cookie policy here.

4. Social media activities

We have various presences in social networks to communicate with users active there and to inform them about our services. For example, we use icons that lead to the pages of Youtube, Linkedin or Facebook. For more information about this and about the use of cookies, please see our Cookie Policy here.

D. International data transfers

Whenever possible and economically justifiable, Yokoy endeavors to work with providers from Switzerland, the EEA or the EU, or with countries for which the Federal Council persuant Art. 16 Para. 1 RevFADP or EU Commission has recognized an adequate level of data protection pursuant to Art. 45 GDPR.
Alternatively, the data transfer takes place on the basis of standard contractual clauses pursuant to Art. 16 Para. 2 lit. b RevFADP or Art. 46 GDPR. We are aware that the ruling of the European Court of Justice C-118-311 of 16.7.2021 has declared the Privacy Shield null and void and requires our sub-processors to implement the new standard contractual clauses published by the EU Commission on 4 June 2021. We are following developments in this regard very closely, particularly with regard to an adequacy decision by the EU Commission. This is currently in the draft stage. Such an adequacy decision would enable data transfer without additional measures. As this is not the case at the moment, we base our data transfers in the non-EU area on the standard contractual clauses together with the additional measures taken by the sub-processors. If available at the partner, we base the data transfer on Binding Corporate Rules according to Art. 16 Para 2 lit. e RevFADP or Art. 47 GDPR.

Yokoy has conducted an internal Data Transfer Impact Assessment. Based on the data processed by Yokoy, the security measures taken by us and our partners, we conclude that the risk of data access by the US authorities based

on US national security interests is to be assessed as very low. An internal process has been established for the event of a request from the authorities. To date, there has never been such a request since our company was founded in 2019.

We work exclusively with large international partners who share our conviction regarding the importance of data protection. The guarantee of data protection is additionally contractually ensured by data processing agreements with our partners and suppliers.

Our multi-stage procurement process includes separate clarifications on the topics of data protection and data security. Below is an overview of our foreign partners, in which country they are located and for what purpose they process Yokoy data. In addition, an internal policy states that we support any international sanctions against states, territories or persons and do not have business relationships with such states, territories or persons. The partners who explicitly process customer data are listed in the Data Processing Addendum, which is part of the customer relationship contract.

Sub-processor	Location	Basis of the data transmission	Purpose of processing	Technical and organisational measures	Address
Google LLC, Ireland	EU (St. Ghislain, Belgium Frankfurt	SCC and additional measures	Use of cloud services for data storage (Google Cloud) in Europe, hosting of Yokoy software (Google Cloud Web Hosting), email communication (Gmail) and document management (G Suite), and data management (BigQuery).	Google trust center	Google Ireland LLC Gordon House Barrow Street Dublin 4, D04E5W5 Ireland
WordPress	USA	SCC and additional measures	Website hosting https//www.yokoy.ai on the basis of Art. 6 Para. 1 lit. b and f GDPR	Wordpress security	Automattic Inc. 60 29th Street #343 San Francisco, CA 94110 United States of America

Hubspot Germany GmbH	Frankfurt	SCC and additional measures	Hubspot is also used for marketing and communication purposes based on your consent pursuant to Art. 6 (1) a GDPR or Art. 6 (1) b GDPR for the performance or preparation of a contract and Art. 6 (1) f GDPR for our legitimate interests (in particular marketing).	Hubspot trust center	HubSpot Germany GmbH AM Postbahnhof 17 10243 Berlin
Sendgrid LLC, Denver (optional can be deactivated)	USA	SCC and additional measures	Sending platform emails - the employee's email is shared with Sendgrid.	Sendgrid security	1801 California Street Suite 500, Denver, CO 80202 USA respectively Twilio, Inc. 375 Beale Street Suite 300 San Francisco, CA 94105 USA
Intercom, Dublin	Dublin	SCC and additional measures	In-app chat function, Yokoy Academy, user data analytics for product development and direct customer communication. The analytics part can be disabled upon request.	Intercom security	3rd Floor, Stephens Ct., 18-21 St. Stephen's Green, Dublin 2

Slack Technologies, Inc.	USA	SSCC and additional measures	Web-based instant messaging for internal corporate communication	Slack security	Slack Technologies, Inc, 500 Howard Street, San Francisco, CA 94105, USA.
ProspectOne	Poland	Adequacy decision pursuant to Art. 45 GDPR	For the provision of a CDN (Content Delivery Network). No personal data is requested or stored.	jsdelivr Privacy and Security	JS Deliver, ProspectOne, Królewska 65A/1, 30-081, Kraków, Poland.
Microsoft Corporation	USA	SCC and additional measures	Use of cloud services for customer communications (Microsoft Teams Microsoft Azure internal Access Management).	Microsoft security	Microsoft Corp. One Microsoft Way, Redmond, WA 98052-6399, USA
DocuSign Germany GmbH	Germany	Binding corporate rules pursuant to Art. 47 GDPR.	Electronic signing of contracts on the basis of Art. 6 Para.. 1 lit. b GDPR	Docusign security	DocuSign Germany GmbH New Rothofstrasse 13-19 60313 Frankfurt Germany
Aircall, Inc.	France	SCC and additional measures	Cloud-based call center software based on Art. 6 Para I lit. b and lit. f	Aircall security	Aircall, Inc. 11 Rue Saint-Georges, 75009 Paris, France

Hypothekarbank Lenzburg	Switzerland	Adequacy decision pursuant to Art. 45 GDPR	Establishment and management of the billing account and thus necessary fulfillment of legal requirements (pursuant to Art. 6 Para. I lit. b, c and f) GDPR). Furthermore, for the purpose of issuing the Yokoy Card and the associated legal requirements (pursuant to Art. 6 Para. I lit. b, c and f) GDPR).	Hypothekarbank Lenzburg Security	Hypothekarbank Lenzburg Bahnhofstrasse 2, 5600 Lenzburg, Switzerland.
Exceet Card Group	Germany	SCC and additional measures	Processing and authorization of transactions for the Swiss Yokoy corporate card.	Exceet security	Exceet Card Group, Edison Strasse 3, 85716 Unterschleissheim
Cookiebot	Danmark	SCC and additional measures	Cookie management tool on our website.	Cookiebot TOMS	Havnegade 39, 1058 Copenhagen, Denmark
Salesforce Ireland Ltd.	Ireland	BCR+SCCs	CRM	Salesforce security	One Central Park Level 3 Central Park Leopardstown Dublin 18

Atlassian	Netherlands	SCC and additional measures	Development and ticketing tool	Atlassian security	Atlassian B.V. Singel 236, 1016 AB Amsterdam
Cognism	England	SCC and additional measures	Prospecting Tool	Cognism security	Cognism Inc. TOG Borough Yards, 13 Dirty Ln, London SE1 9PA
Dealfront	Germany	SCC and additional measures	Prospecting Tool	Dealfront security	Dealfront Durlacher Allee 73 76131 Karlsruhe
The following subprocessors are only used in connection with the Yokoy Pay program					
Modulr Finance B.V.	Netherlands	SCC and additional measures	E-Money Institution Account Provider (Yokoy Pay) For EU Customers	Modulr security	Modulr Finance B.V. Weteringschans 165C, 1017 XD, Amsterdam
Modulr Finance Limited	UK	SCC and additional measures	E-Money Institution Account Provider (Yokoy Pay) For UKCustomers	Modulr security	Modulr Finance Limited, Scale Space 58 Wood Lane, London W12 7RZ

Transact Payment Malta Limited	Malta	SCC and additional measures	BIN Sponsor (Licensor Visa) for EU customers	PCI-DSS certificate available	Transact Payments Malta Limited Vault 13-15, Valletta Waterfront, Pinto Wharf, Valletta, Malta, FRN 1913
Transact Payment Limited	UK	SCC and additional measures	BIN Sponsor (Licensor Visa) for UK customers	PCI-DSS certificate available	Unit 5.1, Level 05 Madison, Midtown Queensway Gibraltar GX11
Marqeta, Inc	USA	SCC and other measures	Processor of card transactions	Marqeta security	Marqeta, Inc. 180 Grand AVE 6th floor Oakland, CA 94612
Tag Systems UK ltd	United Kingdom	Adequacy decision according to Art. 45 GDPR	Physical production of the cards	Extensive security policy can be provided upon request	Tag Systems UK ltd 32 Marathon Pl, Moss Side Industrial Estate, Leyland PR26 7QN, United Kingdom

E. Data security

Data security is a very important concern for us, as we are a fintech company operating in a sensitive area, we are aware of our responsibility. This is also the reason for this comprehensive privacy policy. Yokoy is certified by TÜV Rheinland according to the IT security standard ISO 27001. Furthermore, an external company tests the security of our software annually in so-called penetration tests. The recommendations are recorded and implemented in order to further improve the already high security standards in the future according to the ISO principle of continuous improvement and to have them independently verified. A quality management system according to the

specifications of ISO 9001 and an environmental management system according to the specifications of ISO 14001 is implemented and certified by Attesta Schweizer Zertifizierungsgesellschaft AG in March 2023.

I. Physical security

Access to the building and offices is only granted via a badge system, which is personally issued by the supervisor. For better traceability, entries and exits to the engineering offices are also logged. There is an internal physical security policy that is included in regular employee training.

II. Access

Access to our online offer takes place via transport encryption (SSL / TLS, in particular with the Hypertext Transfer Protocol Secure, abbreviated HTTPS). Most browsers indicate the transport encryption by a padlock in the address bar.
Even when the data is with us, it is in good hands. We chose Google Cloud Platform as our cloud provider because Google has always evolved in terms of data security and offers us a reliable service. Google's collaboration with SAP ensures high data availability. The security and data protection of Google products are independently audited on a regular basis (ISO/IEC 27001, 27017, 27018, SOC 1/2/3, GDPR). An overview of all certifications is available here: Google Cloud Compliance

The data in the cloud is encrypted with a 256 AES (Advanced Encryption Standard) and all data is also encrypted during transmission. The storage of the data is contractually assured in the EU (Frankfurt, St. Ghislain, Belgium and Zurich) and the keys for encryption are held by Yokoy. An internal encryption policy is in place and is part of regular employee training.

III. Access management

Access is based on the need-to-know principle and is role-based. All activities are logged in order to be able to verify and prove access to the data. In addition, all access management issues are documented in an internal policy. All employees are also subject to a confidentiality obligation.

IV. Data availability

The data is provided on demand and automatically backed up every 24 hours in an encrypted cloud (storage period 30 days), so that the data is available at all times. The multi-tenant infrastructure also ensures that the data is available even if an incident were to occur at a specific data center and it were to be unavailable for a short time. A good overview of the security measures in a typical Google Cloud data center can be found here Security in the Google Datacenter.

V. Emergency plan

If, despite all measures, a data incident should occur, we are prepared for it and will put our internal emergency plan into action to inform customers and partners and minimize the damage.

F. Data storage and deletion

We respect your data and store it only as long as it is absolutely necessary for the intended purpose (principle of data minimization according to Art. 5 lit. c GDPR and Art. 6 Para. 3 RevFADP. In case of data provided to us by you as part of an order, we delete the data in accordance with the specifications of the order. Personal data is only collected, processed and used to the extent that it is necessary for the establishment, content or modification of the legal relationship (inventory data). This is done on the basis of Art. 6 Para. 1 lit. b GDPR, which allows us to process data for the fulfillment of a contract or pre-contractual measures. At the request of the customer, the data will also be stored in our archive for a longer period of time, e.g. for an audit or for a tax audit, based on a specially set up audit role with read-only rights. The right to deletion according to Art. 17 GDPR is always reserved, provided that the legal requirements for this right are met. In addition, we store daily backups of our data in order to comply with the principle of data availability. The backup data is automatically deleted after 30 days. The procedure for data storage and data deletion is documented in an internal policy.

G. Your rights

1. Right to confirmation Art. 25 Para 1 revFADP Art. 15 GDPR

On the basis of Art. 25 Para 1 revFADP and 15 GDPR you have the right to request confirmation from us as to whether personal data relating to you is being processed. To do so, please contact us via the above contact person.

2. Right to information Art. 25 Para 2 revFADP and Art. 15 GDPR

In accordance with Art. 15 GDPR and Art. 8 Para. 1 FADP, you also have the right to receive from us at any time and free of charge information about the data stored about you and a copy of this data in accordance with the legal provisions. To do so, please contact us via the contact person above. This data is provided in JSON or .csv format.

3. Right to rectification Art. 32 revFADP and Art. 16 GDPR

You have the right to request the rectification of inaccurate personal data concerning you. You also have the right to request that incomplete personal data be completed, taking into account the purpose of the processing. The obligation to keep the employee user master data up to date lies with the customer, as we receive this data from the customer and are not in a position to verify it.

4. Right to erasure Art. 6 Para. 4 RevFADP and Art. 17 GDPR

You have the right to demand that we delete the personal data concerning you without delay, provided that one of the reasons provided for by law applies and insofar as the processing or storage is not necessary. To do so, please contact us via the above contact person. The FADP does not specifically grant a right to erasure but Art. 6 Para. 4 revFADP is requesting the destruction or anonymization of data which are no longer necessary to fullfill the purpose.

5. Restriction of processing Art. 6 Para. 3 RevFADP and Art. 18 GDPR

You have the right to request that we restrict processing if one of the legal requirements is met. To do so, please contact us via the contact person above. This right is not explicitly granted in the FADP but it is covered by the purpose limitation stipulated in Art. 6 Para. 3 RevFADP.

6. Obligation to notify Art. 9 Para. 3 RevFADP and Art 19 GDPR

Yokoy will communicate changes, deletions and restrictions of data processing to third parties, unless this proves impossible or involves a disproportionate effort. Art. 9 Para. 3 FADP require this in specific case of the engagement of a new subprocessor. If we do so, customers are informed with a notice preiod of 15 days as stipulated in the Data Processing Agreement.

7. Data portability Art. 28 revFADP and Art. 20 GDPR

You have the right to receive the personal data concerning you that you have provided to us in a structured, common and machine-readable format. We provide the data in .csv or JSON format. You also have the right to transfer this data to another controller without hindrance from us, to whom the personal data has been provided, provided that the processing is based on consent pursuant to Art. 6 Para. 1 lit. a GDPR or Art. 9 Para 2 lit. a GDPR or on a contract pursuant to Art. 6 Para. 1 lit. b GDPR and the processing is carried out with the aid of automated procedures, unless the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us.

Furthermore, when exercising your right to data portability pursuant to Article 20 Para I GDPR, you have the right that the personal data be transferred directly from one controller to another controller, to the extent technically feasible and provided that this does not adversely affect the rights and freedoms of other individuals. For this purpose, the data may be provided in .CSV or .JSON format. To do so, please contact us via the contact person above. The right to data portability is also granted in Art. 28 revFADP, but restrictions apply mainly on fesability and proportionalit

8. Objection Art. 21 GDPR

You have the right to object at any time, on grounds relating to your particular situation, to the processing of personal data concerning you that is carried out on the basis of Art. 6 Para. 1 lit. e or lit. f GDPR. This also applies to profiling based on these provisions within the meaning of Art. 4 No. 4 GDPR.
If you object, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is necessary for the establishment, exercise or defense of legal claims.

In individual cases, we process personal data in order to conduct direct advertising. You may object to the processing of personal data for the purpose of such advertising at any time. This also applies to profiling, insofar as it is associated with such direct advertising. If you object to the processing for direct marketing purposes, we will no longer process the personal data for these purposes.
You also have the right to object, on grounds relating to your particular situation, to the processing of personal data concerning you which is carried out by us for scientific or historical research purposes or for statistical purposes pursuant to Art. 89 Para. 1 GDPR, unless such processing is necessary for the performance of a task carried out in the public interest.
Notwithstanding Directive 2002/58/EC, you are free to exercise your right to object to the use of information society services by automated means using technical specifications. To do so, please contact us via the contact person above.

9. Revocation of consent under data protection law

You have the right to revoke your consent to the processing of personal data in accordance with Art. 7 Para. 3 GDPR at any time with effect for the future. To do so, please contact us via the contact person above.

10. Complaint to a supervisory authority

You have the right to lodge a complaint about the processing of personal data by us with a supervisory authority responsible for data protection in accordance with Article 77 of the GDPR. In Switzerland, our supervisory authority is the Federal Data Protection and Information Commissioner (FDPIC):

The Federal Commissioner for Data Protection and Freedom of Information
Feldeggweg 1
CH - 3003 Bern
Phone: +41 (0)58 462 43 95 (Mon. to Fri., 10.00 to 12.00)
Fax: +41 (0)58 465 99 96

For data subjects from the EU area, our lead supervisory authority is

Bavarian State Office for Data Protection Supervision (BayLDA)
Promenade 18
91522 Ansbach
Phone: +49 (0) 981 180093-0

H. Updates

We can adapt and supplement this data protection declaration at any time. We will inform you about such adjustments and additions in an appropriate form, in particular by publishing the respective current data protection declaration on our website.