



# A practical guide to using OnceHub in a GDPR compliant manner



# Table of Contents

<b>Glossary</b>	<b>2</b>
<b>Background</b>	<b>4</b>
What does the GDPR mean for OnceHub users?	4
<b>Lawful basis for processing</b>	<b>5</b>
Scheduling under a generic configuration	5
Personalized scheduling	6
Collection of sensitive data	6
<b>Accountability</b>	<b>10</b>
Demonstrating compliance	10
Maintaining records	10
<b>Data protection officer and EU representative</b>	<b>12</b>
Data Protection Officer	12
EU representative	12
Providing contacts to OnceHub	13
<b>Data protection by design and default</b>	<b>14</b>
Collecting data from individuals who schedule meetings	15
Securing your OnceHub account	17
Accessing customer data	19
<b>Data subject rights</b>	<b>25</b>
The right to access data	26
The right to rectification	29
The right to erasure	29
<b>Data protection impact assessments and breach notifications</b>	<b>29</b>
<b>We are here to help!</b>	<b>30</b>

We have created this practical guide to help you ensure your use of OnceHub's products is compliant with the GDPR. If you are already using OnceHub, you have agreed to our [Data Processing Addendum](#). Agreeing to the DPA is just one step in the road to GDPR compliance. Read this guide for tips and insights on setting up and using your OnceHub account according to the principles outlined in the GDPR.



***Disclaimer:*** This practical guide is designed to help our users understand the GDPR in relation to OnceHub's platform. The information contained herein should not be construed as a comprehensive solution or legal advice. Each organization should take its own steps to ensure compliance.

# Glossary

**OnceHub:** The company that owns and develops the online scheduling products ScheduleOnce and InviteOnce. OnceHub is the legal entity that upholds the principles of the GDPR.

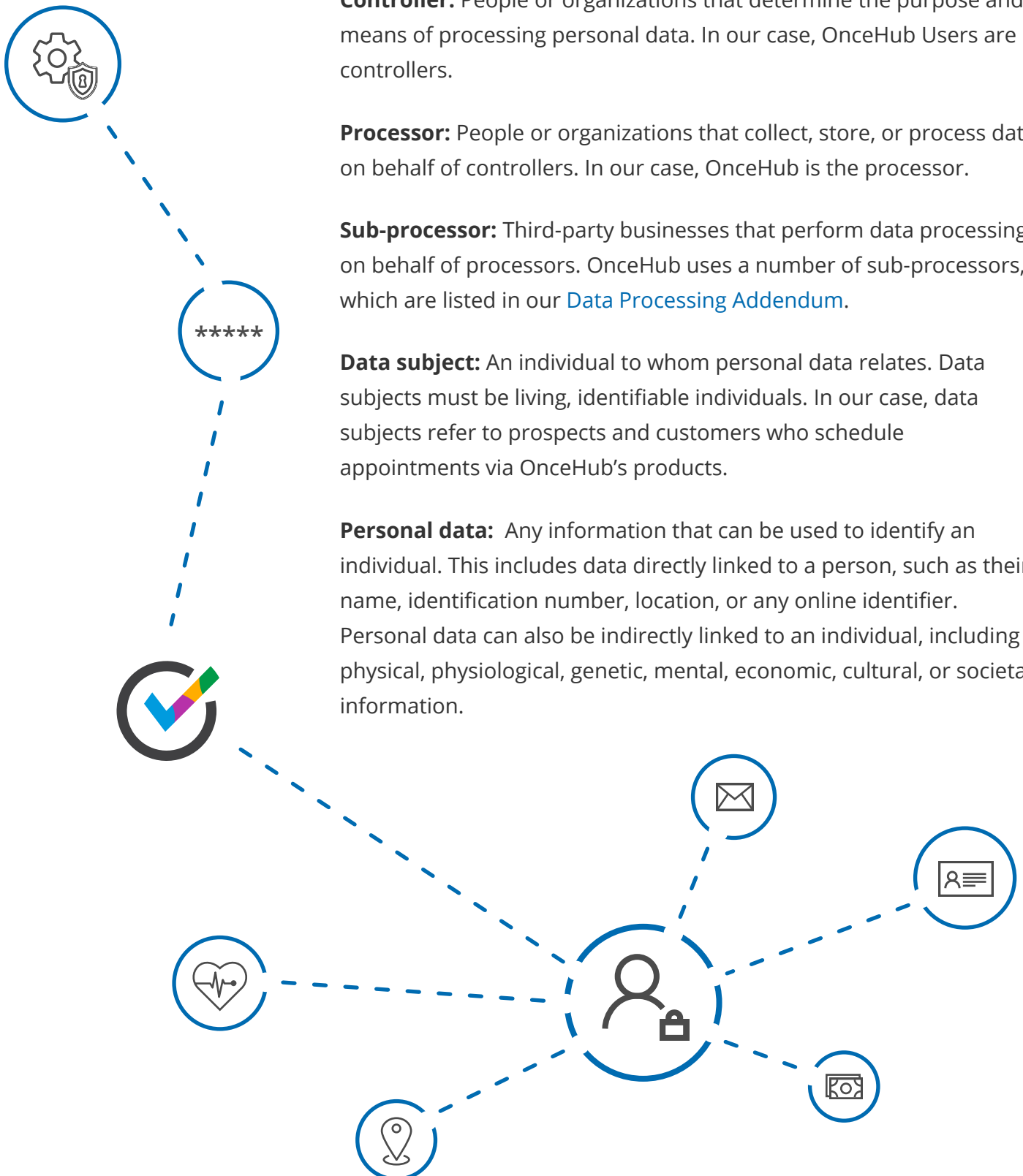
**Controller:** People or organizations that determine the purpose and means of processing personal data. In our case, OnceHub Users are controllers.

**Processor:** People or organizations that collect, store, or process data on behalf of controllers. In our case, OnceHub is the processor.

**Sub-processor:** Third-party businesses that perform data processing on behalf of processors. OnceHub uses a number of sub-processors, which are listed in our [Data Processing Addendum](#).

**Data subject:** An individual to whom personal data relates. Data subjects must be living, identifiable individuals. In our case, data subjects refer to prospects and customers who schedule appointments via OnceHub's products.

**Personal data:** Any information that can be used to identify an individual. This includes data directly linked to a person, such as their name, identification number, location, or any online identifier. Personal data can also be indirectly linked to an individual, including physical, physiological, genetic, mental, economic, cultural, or societal information.



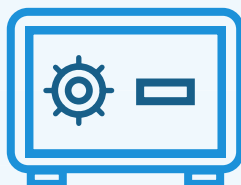
**Processing:** Any operation performed on personal data. This includes automated and manual operations such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating, making available, combining, restricting, erasing or destroying.

**Data Processing Addendum (DPA):** A contractual agreement between two organizations outlining terms and responsibilities for data protection.

**Data protection officer:** A position within an organization responsible for ensuring the security and protection of data. A DPO can be an employee of an organization, or be retained as a contracted service.

**EU representative:** A person or organization designated by a controller or processor located outside of the EU to represent the controller in EU member states. The EU representative is responsible for GDPR compliance and can act on behalf of the controller. Supervisory authorities may address the EU representative in place of the controller or processor.

**Supervisory authority:** An independent public authority established by an EU member state to enforce the GDPR. Each member state has its own supervisory authority.



# Background

The GDPR is the European Union's new data protection law that unifies the different privacy legislation across EU member states. This new framework replaces the current EU Data Protection Directive (Directive 95/46/EC).

**The purpose of the regulation is to strengthen the privacy rights of individuals in regards to how their personal data is being collected, processed, and used.**

To protect personal data, the GDPR requires organizations to implement operational and technological controls. These controls cover:

1. How data is collected
2. The use of the collected data
3. Storage of the data
4. Individual's rights to their data

Any organization, no matter its location, must comply with the GDPR in order to process or monitor the data of EU residents. Additionally, organizations are accountable for demonstrating their compliance with the GDPR and maintaining records of processing activities to that effect.

*Penalties for non-compliance are significant. Organizations that do not comply can be fined up to 4% of annual global turnover or €20 million, whichever is higher.*

The regulation applies to organizations that offer products or services to, or monitor data of EU residents. Under the GDPR, these organizations are called controllers. It also applies to processors and sub-processors used to collect and store information on behalf of controllers.

## What does the GDPR mean for OnceHub users?



GDPR compliance requires commitment from both OnceHub and its users. OnceHub is committed to being a trusted vendor and to protecting your customer data. As the processor of customer data, we work closely with privacy experts to ensure our privacy and security programs meet the standards outlined in the GDPR.

This guide covers the key requirements outlined in the GDPR that relate to the use of OnceHub's products. Follow this guide to learn what you can do to ensure you are upholding your responsibilities.



## Lawful basis for processing

Under the GDPR, controllers must have a lawful basis for processing information ([Article 6](#)). With scheduling, establishing a lawful basis for processing depends on who inputs the data of the individual being scheduled. If you offer scheduling under a generic configuration, your customers are required to input their information. According to Article 6.1 b, this in itself provides you with a lawful basis for processing their information as they are the ones taking the initiative to schedule with you. Alternatively, scheduling can be personalized, meaning you input the data of the individual being scheduled. To do this, you need to have their consent or other lawful basis.

### Scheduling under a generic configuration

This scenario occurs when a customer schedules from a booking page with a generic configuration. This means that the customer is not identified in advance, and is therefore required to input their name and email in order to schedule the meeting. This is only relevant if you are using ScheduleOnce. Under the GDPR, you can process information if it is necessary to fulfill a business obligation to a prospect or customer. In this scenario, when a prospect or customer inputs their information to schedule a meeting, you need to process their information to fulfill your business obligation. For most organizations, this should be enough to ensure a lawful basis for processing information.




## Personalized scheduling



Personalized scheduling is when you input the information of a specific prospect or customer who you are scheduling with. This is relevant for both ScheduleOnce and InviteOnce. With ScheduleOnce, you may personalize scheduling by sending [personalized links](#) to prospects or customers. In this scenario, customer data is pulled from [Salesforce](#), [Infusionsoft](#), or [URL parameters](#). With InviteOnce, scheduling is always personalized because you are required to input the prospect or customer's information while configuring the scheduling requirements. With personalized scheduling, information is processed by OnceHub without any direct input or consent from customers. While your organization may have a lawful basis for processing this data via other sources, it is recommended that you ensure that you have a basis for processing the information via OnceHub.

## Collection of sensitive data

If you are using ScheduleOnce, and require customers to input sensitive data, it is recommended that you obtain explicit consent at the time of scheduling. This most likely applies to organizations in the healthcare industry, but other organizations may be affected as well. Data that is considered sensitive includes any information related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, genetic or biometric data, health information, or a person's sex life or sexual orientation ([Article 9](#)).



☒ I agree  
☐ I disagree

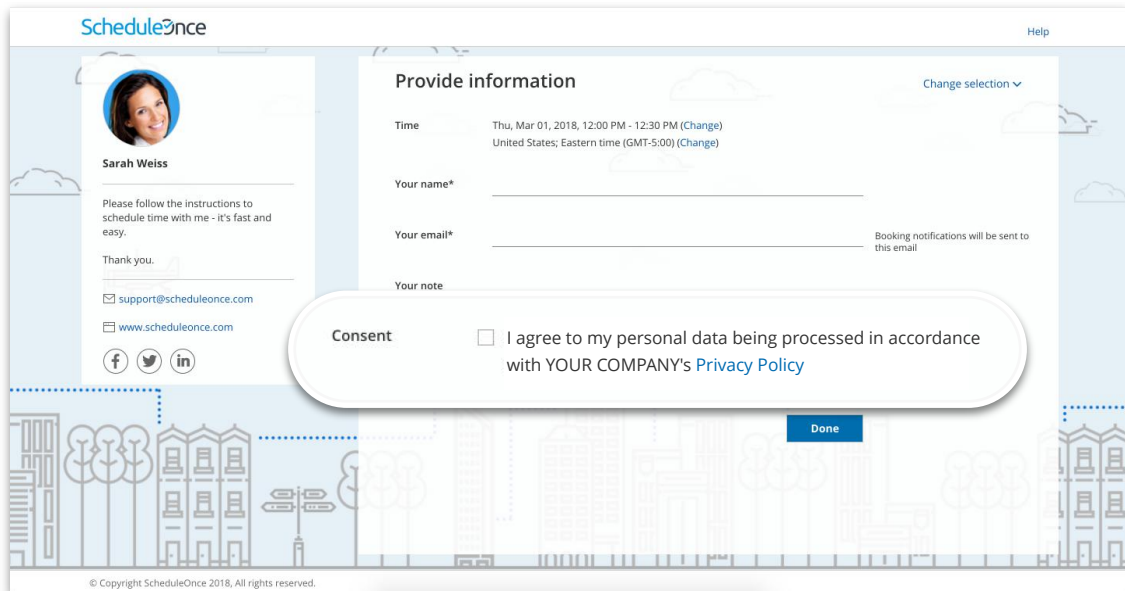
## Obtaining consent for processing

The GDPR defines consent as “freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.” Controllers that process on the basis of consent, must clearly request consent and enable data subjects to withdraw consent at any time ([Article 7](#)). The GDPR also states that if your request for consent occurs in the context of other matters, you should ensure that the request for consent is distinguishable from the other matters.



In order to obtain clear consent for OnceHub to process the data, it is recommended that you add a field in your ScheduleOnce booking form to request consent (See Figure 1).

Figure 1: Consent requested in the booking form

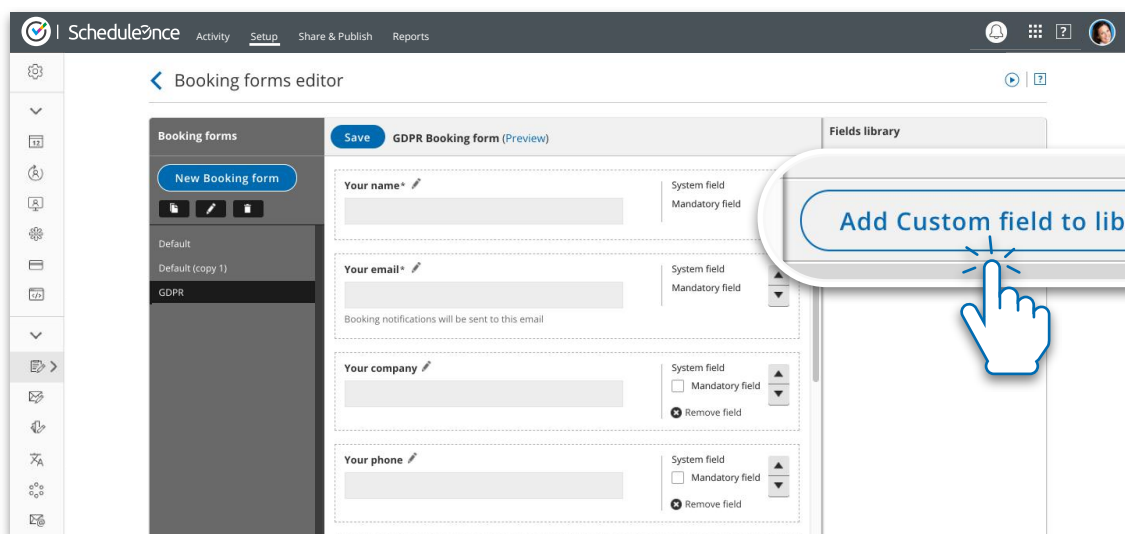


The screenshot shows a booking form titled "Provide information" with fields for Time, Your name\*, Your email\*, and Your note. A "Consent" overlay is displayed in the center, containing the text: "I agree to my personal data being processed in accordance with YOUR COMPANY's [Privacy Policy](#)". The overlay has a "Done" button at the bottom right. The background shows a user profile for Sarah Weiss and a "Change selection" dropdown.

## Steps to request consent during scheduling with ScheduleOnce

1. Go to the Booking forms editor and click **Add Custom field to library** (See Figure 2).

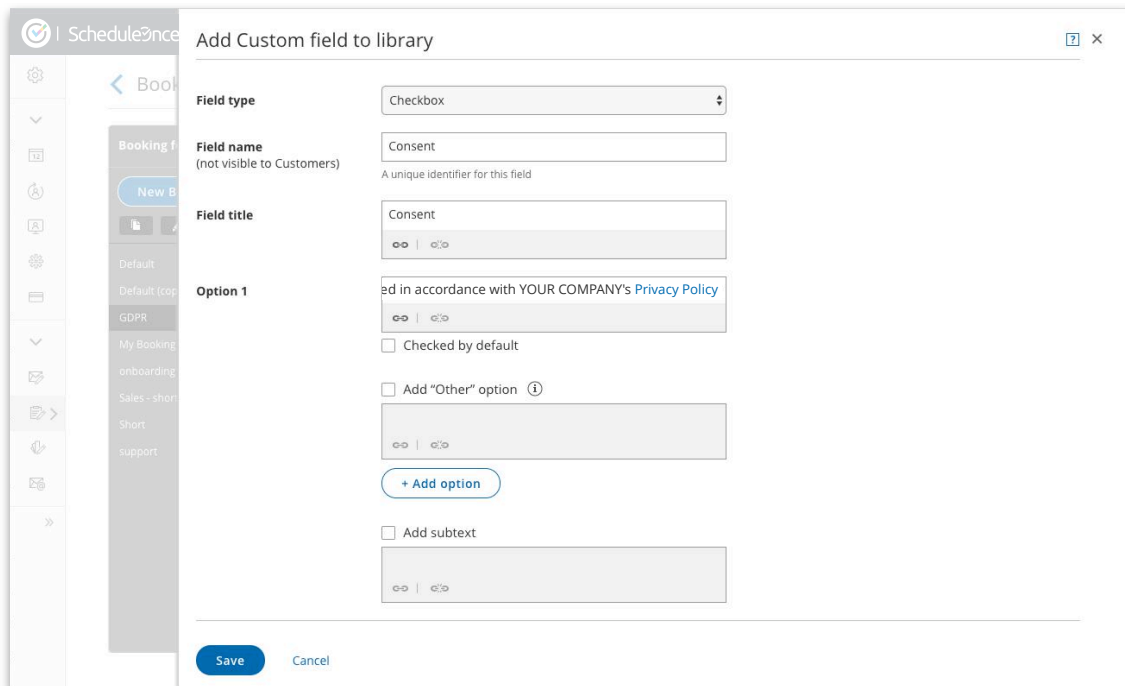
Figure 2: The Booking forms editor



The screenshot shows the "Booking forms editor" interface. On the left, there is a sidebar with a "New Booking form" button and a list of forms: Default, Default (copy 1), and GDPR. The main area displays a "GDPR Booking form (Preview)" with fields for "Your name\*", "Your email\*", "Your company", and "Your phone". Each field has a "System field" dropdown menu with options for "Mandatory field" and "Remove field". A "Fields library" panel is on the right, and a callout bubble with a hand icon points to the "Add Custom field to library" button.

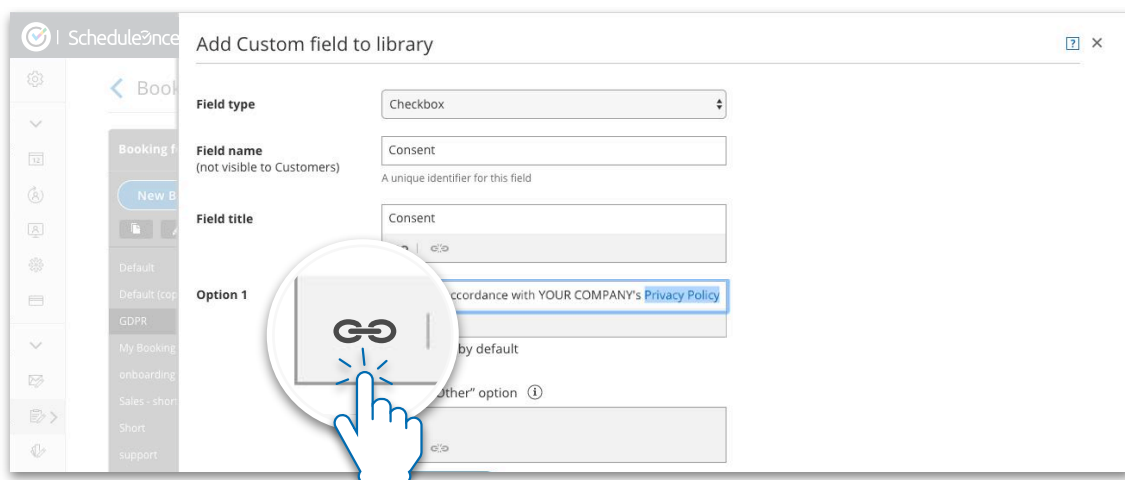
2. Create the Custom field by selecting the Field type, Field name, Field title and Option. We recommend using a Checkbox as the Field type, and creating one option allowing users to provide consent (See Figure 3).

Figure 3: Add Custom field to library



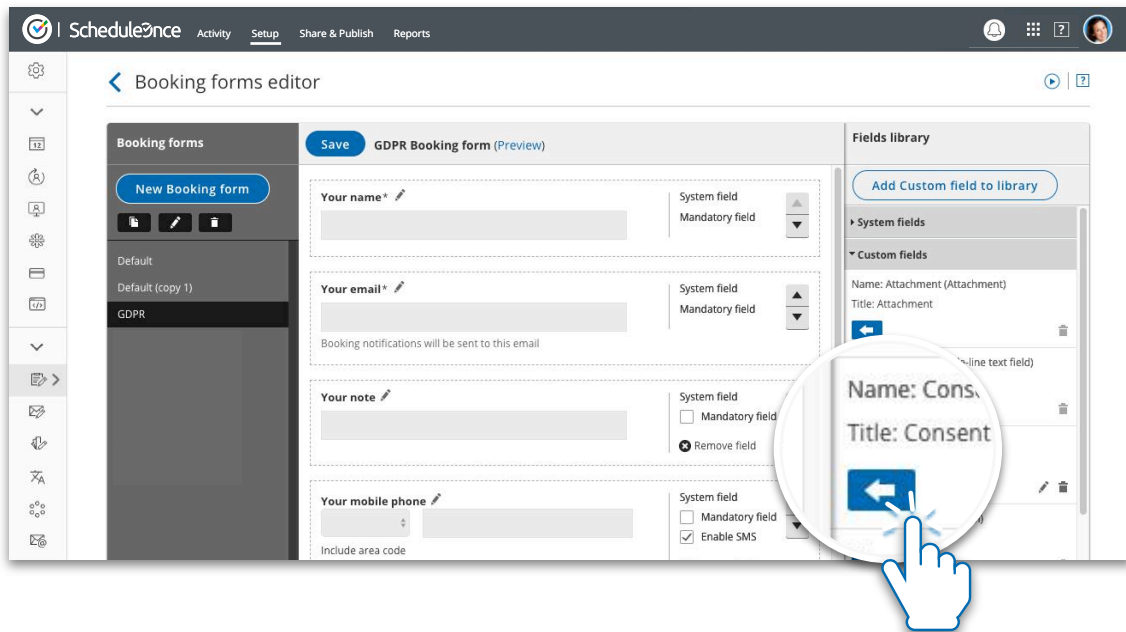
3. When creating your custom field, we recommend linking to your organization's privacy policy. This ensures your customers understand the processing activities to which they are agreeing. To link to the field, highlight the words you want to link and select the link icon (See Figure 4).

Figure 4: Link to your company's privacy policy



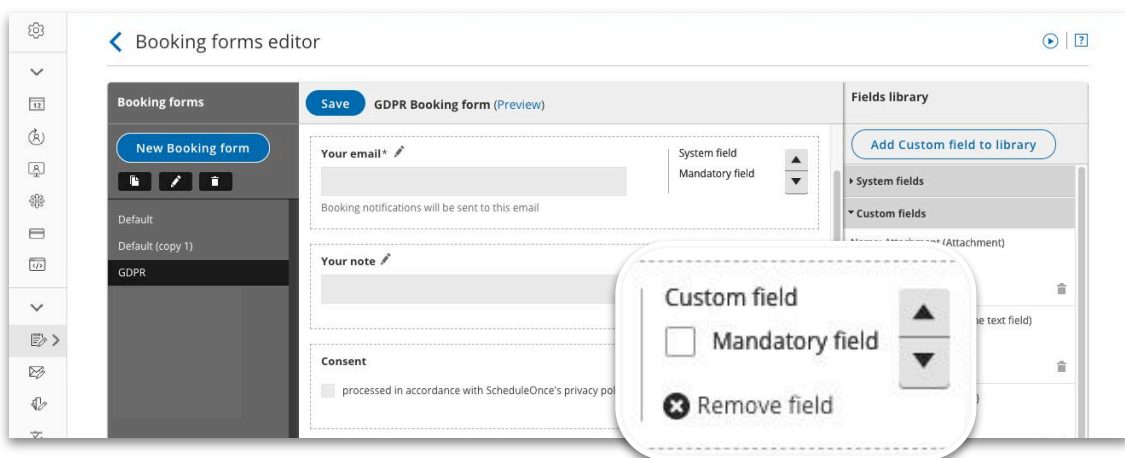
4. Input the link to your privacy policy and press save.
5. Once you have created the field, add it to your booking form by locating the field in the custom fields library and clicking the arrow to add it to the form (See Figure 5).

Figure 5: Add the field to the booking form



6. Next, you can determine the position of the field and whether or not it will be mandatory for customers to check. It is recommended that this field be mandatory (See Figure 6).

Figure 6: Determine the position and whether the field is mandatory



**You are all set!** Your booking form now requests consent for processing data. Be sure to attach this booking form to the relevant booking pages or event types.

# Accountability

Controllers are accountable for demonstrating their compliance with the GDPR ([Article 24](#)). This means that controllers must be able to show that they have taken the necessary steps to ensure their compliance, and done their due diligence regarding the compliance of their processors. Additionally, controllers are accountable for maintaining records of their processing activities, and must provide information to their processors regarding their processing activities ([Article 30](#)).

## Demonstrating compliance



To demonstrate that you have done your due diligence regarding the use of OnceHub's products as your processor, we recommend that you keep a copy of our [Master Service Agreement](#) and [Data Processing Addendum](#) on hand. You may also request access to our [SOC 2 report](#) by [contacting us](#).

Additionally, if you integrate your OnceHub account with any applications, including your calendar, CRM, web conferencing tool, PayPal, or any other app via Zapier, you are responsible for ensuring that all vendors accessing your OnceHub data are GDPR compliant.

## Maintaining records

Controllers must maintain records of their processing activities. Information that must be recorded includes:

- ⦿ The purpose of processing
- ⦿ A description of the categories of personal data being processed
- ⦿ A description of the categories of data subjects whose data is being processed



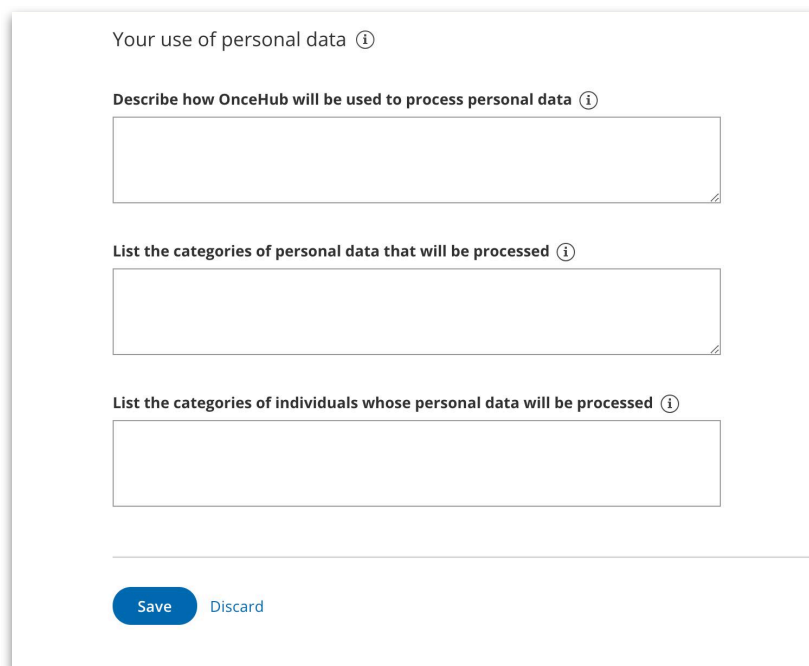
While the GDPR states that organizations with less than 250 employees may not need to keep full records of their processing activities, OnceHub recommends that you maintain records to the best of your abilities.

To facilitate compliance, you should provide this data to OnceHub.

## Setup steps

1. To provide OnceHub with records of your processing activities, go to Account > Privacy > GDPR information.
2. Fill out the section **Your use of personal data** (See Figure 7).

*Figure 7: Your use of personal data section*



The screenshot shows a form titled "Your use of personal data" with an information icon. It contains three text input fields, each with a label and an information icon:

- Label: "Describe how OnceHub will be used to process personal data".
- Label: "List the categories of personal data that will be processed".
- Label: "List the categories of individuals whose personal data will be processed".

At the bottom of the form are two buttons: "Save" (in blue) and "Discard" (in grey).

**You're all set!** You have now provided OnceHub with a record of your processing activities.

# Data protection officer and EU representative

Organizations that process data, regardless of whether they are located in the EU, may need to appoint a Data protection officer to monitor internal compliance with the GDPR. Additionally, organizations that are located outside of the EU and are regulated by the GDPR need to appoint an EU representative.

## Data protection officer

The GDPR outlines three cases in which controllers need a DPO:

1. The controller is in the public sector
2. The controller regularly or systematically monitors data on a large scale
3. The controller processes sensitive data on a large scale.

([Article 37](#))



### Do organizations using OnceHub need a DPO?

Having a OnceHub account does not necessarily mean that your organization needs to appoint a DPO. You should examine your organization's core activities to determine whether you meet one of the three cases that would require an appointment of a DPO. That said, appointing a DPO could be very beneficial to your business even if it is not required. As an impartial party, a DPO can help your organization ensure all processing activities are conducted in a GDPR compliant manner. Your DPO can either be an employee of your organization, or be retained as a contracted service.

## EU representative

If your organization is not located in the EU, the GDPR requires that you appoint an EU representative to ensure compliance and represent your organization to the supervisory authority in the EU member states. Your organization may need to appoint an EU representative if you process data on a large scale and are in the private sector ([Article 27](#)).

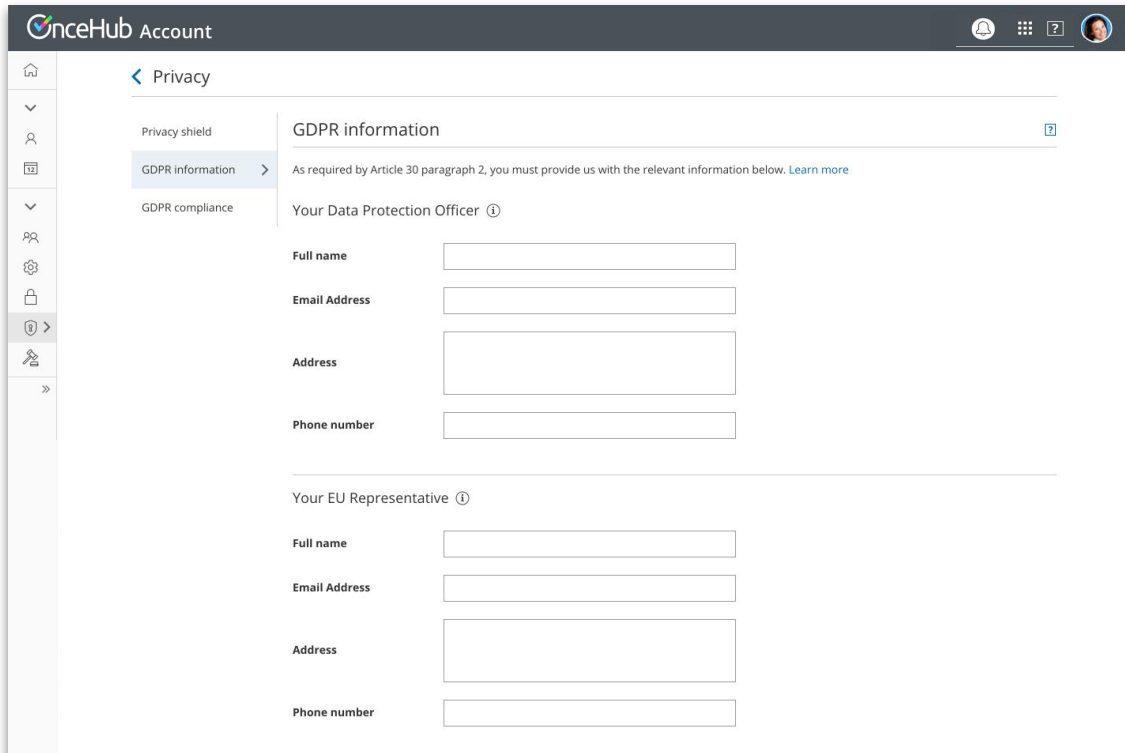
## Providing contacts to OnceHub

The contact details of your DPO and EU representative must be readily available to data subjects, processors and the relevant supervisory authority. To ensure compliance, OnceHub requires that you provide this information in your account settings.

### Steps to add contact information about your DPO and EU representative to your OnceHub account

1. To provide OnceHub with the contact details of your DPO and EU representative, go to Account > Privacy > GDPR information (See Figure 8).

Figure 8: GDPR information section of the Account settings



The screenshot displays the 'OnceHub Account' interface. On the left is a sidebar with navigation icons. The main content area is titled 'Privacy' and contains a sub-section 'GDPR information'. Below this, there are two main sections: 'Your Data Protection Officer' and 'Your EU Representative'. Each section contains four input fields: 'Full name', 'Email Address', 'Address', and 'Phone number'. A 'Learn more' link is visible next to the introductory text for the DPO section.

2. Fill in the information regarding your DPO and EU representative.

**You're all set!** This information can be edited at any time.

# Data protection by design and default

The GDPR lays out two principles regarding how organizations should ensure data protection when determining their processes for collecting and storing information:

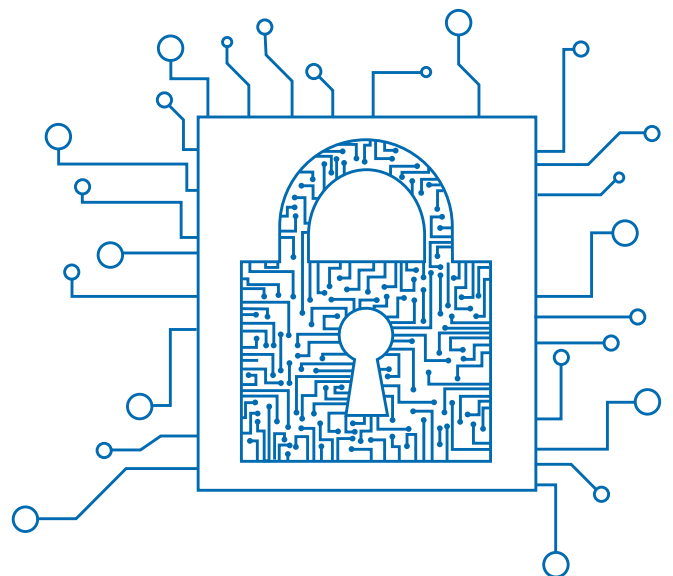
1. Data protection by design
2. Data protection by default

**Data protection by design** states that controllers should “implement appropriate technical and organisational measures” and “integrate the necessary safeguards into the processing.” Controllers should consider data protection both when designing procedures to process information, and at the time of the processing itself ([Article 25](#)).

**Data protection by default** states that controllers should ensure that “by default, only personal data which are necessary for each specific purpose of the processing are processed.” This applies to the amount of personal data collected, the extent of the processing, the period of storage, and the accessibility of the data ([Article 25](#)).

These two principles impact three aspects of using OnceHub’s products:

1. Collecting data from individuals who schedule meetings
2. Securing your OnceHub account
3. Accessing customer data





## Collecting data from individuals who schedule meetings

To uphold the principles of data protection by design and default, you should consider what is the minimum data you require to schedule meetings.

### What data is required to schedule a meeting?

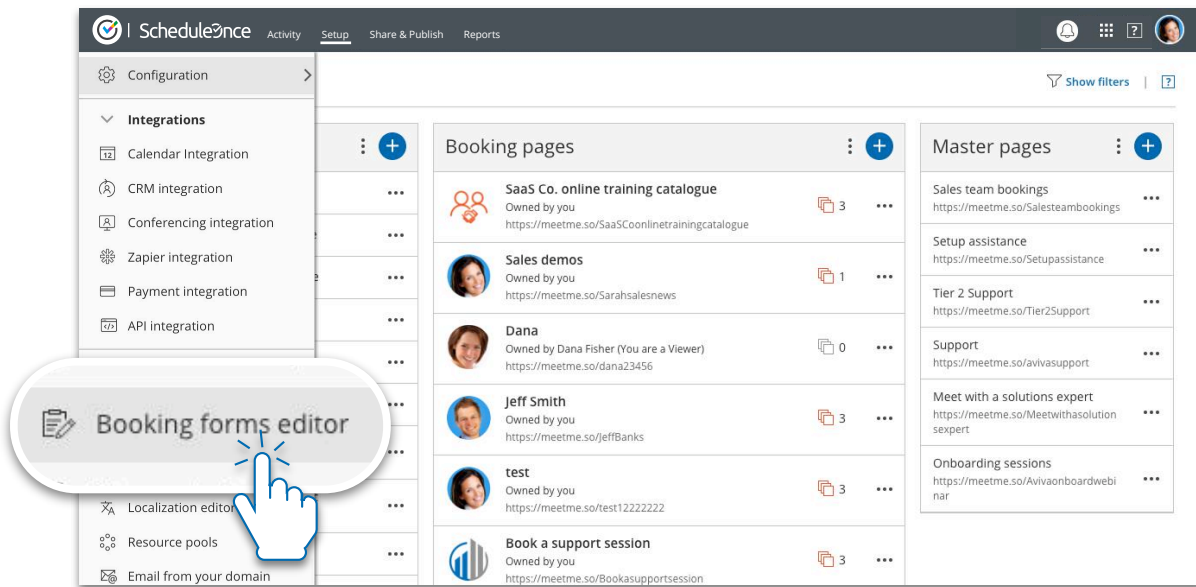
	ScheduleOnce	InviteOnce
<b>Name and email address</b>	This information is required in order for customers to receive confirmation of their booking.	This information is required in order to send scheduling invitations or schedule on a customer's behalf.
<b>Phone number for sending SMS</b>	It is recommended that this field be optional, allowing individuals to decide whether or not they want to receive SMS notifications.	This is not relevant for InviteOnce
<b>Information required for providing your service</b>	Depending on the purpose of your meetings, you may require specific information from individuals to ensure you are prepared for your meeting. Only data that is absolutely necessary for conducting a meeting should be collected.	This is not relevant for InviteOnce

When scheduling with InviteOnce, you already have the customer's details, meaning there is no booking form for the customer to fill out. On the other hand, ScheduleOnce is primarily used to schedule under a generic configuration, meaning you do not have the customer's details and therefore require them to fill out a form. This form can be customized to collect specific information from customers. When customizing booking forms, you should consider compliance with the GDPR. Follow these steps to create custom booking forms with ScheduleOnce.

## Steps to create a custom booking form in ScheduleOnce

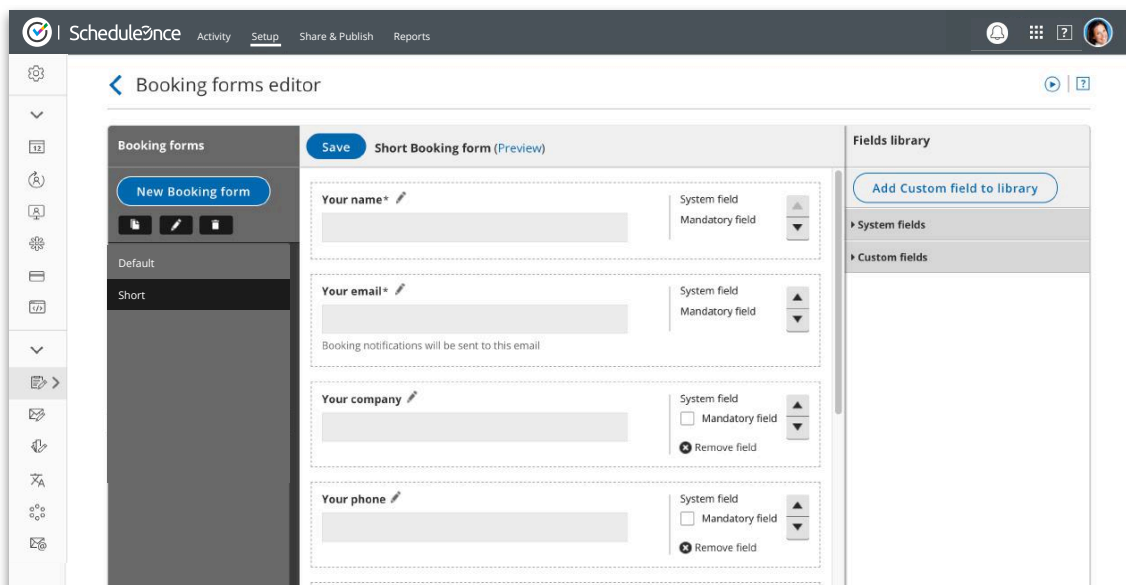
1. In ScheduleOnce, go to the **Booking forms editor** in your account by expanding the left sidebar and selecting the Booking forms editor (See Figure 9).

Figure 9: The Booking forms editor in the left sidebar



2. Using the editor, you can determine which fields your customers will need to fill out in order to book a meeting with you (See Figure 10).

Figure 10: The Booking forms editor



3. Click the “New Booking form” button to create a new form. You can add any fields that you require to your form. ScheduleOnce has a robust library of system and custom fields that you can use. You can also create your own fields if you require other information.
4. Define which fields will be mandatory for customers to fill out and the order in which fields are presented.

**You are all set!** Be sure to associate the booking form to the relevant booking pages and event types.  
[Learn more about the Booking forms editor](#)

## Securing your OnceHub account

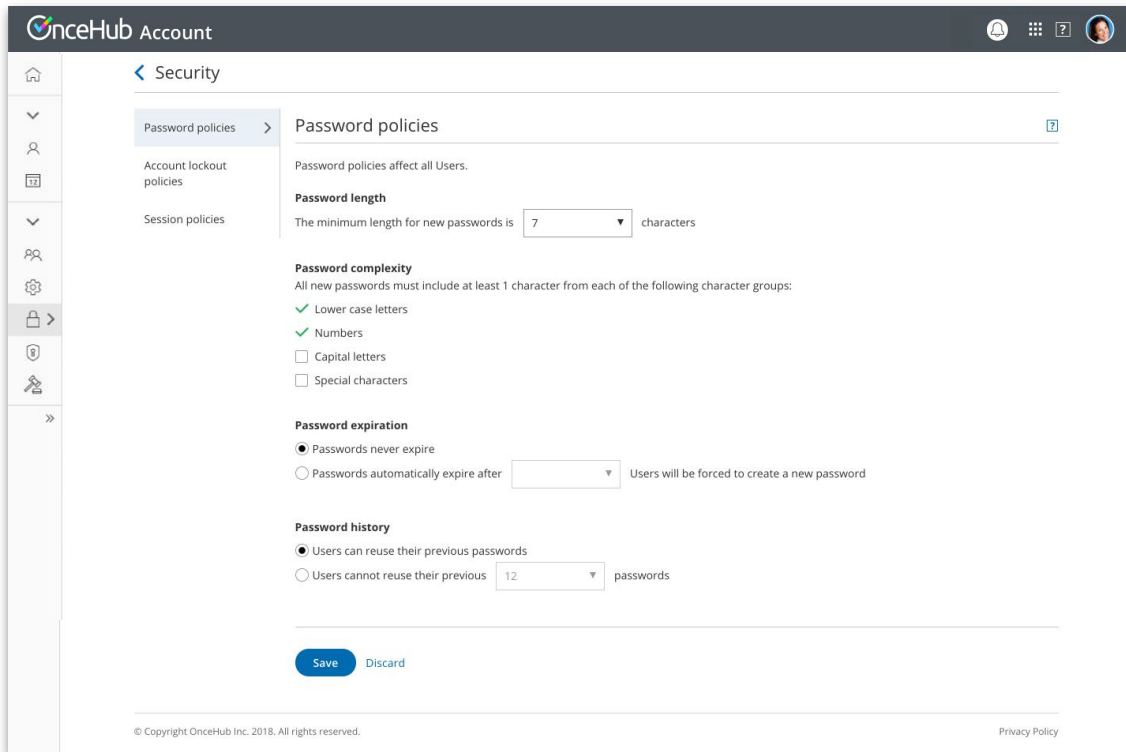
Data protection by design and default require controllers to ensure the security of their OnceHub accounts. By default, OnceHub requires users to use a secure password with at least six characters, including numbers and letters. In addition to our default settings, OnceHub also allows users to set [custom security policies](#) such as stricter password policies, account lockout and short sessions. These additional security policies ensure that you are protecting your account to the highest degree possible.



### Steps to enhance the security of your OnceHub account

1. In your OnceHub account, go to Account -> Security. You will land on the Password policies section (See Figure 11).

Figure 11: The Password policies section of the Security settings



**OnceHub Account**

**< Security**

Password policies

Account lockout policies

Session policies

**Password policies**

Password policies affect all Users.

**Password length**

The minimum length for new passwords is  characters

**Password complexity**

All new passwords must include at least 1 character from each of the following character groups:

- ☒ Lower case letters
- ☒ Numbers
- ☐ Capital letters
- ☐ Special characters

**Password expiration**

☒ Passwords never expire

☐ Passwords automatically expire after  Users will be forced to create a new password

**Password history**

☒ Users can reuse their previous passwords

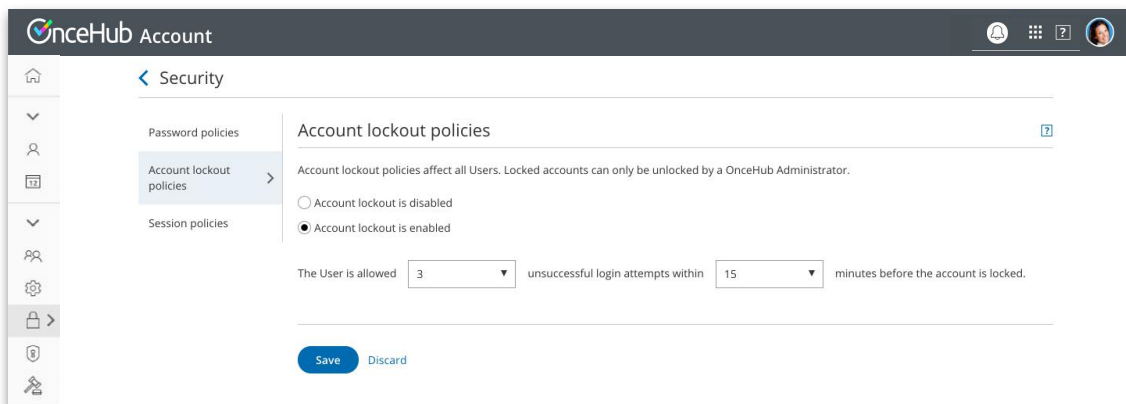
☐ Users cannot reuse their previous  passwords

**Save** **Discard**

© Copyright OnceHub Inc. 2018. All rights reserved. [Privacy Policy](#)

2. Define your password policy. You can set a minimum length, complexity, expiration period, and whether users can reuse their previous passwords. When finished, press Save.
3. Click on the Account lockout policies section (See Figure 12).

Figure 12: Account lockout policies section of the Security settings



**OnceHub Account**

**< Security**

Password policies

**Account lockout policies**

Session policies

**Account lockout policies**

Account lockout policies affect all Users. Locked accounts can only be unlocked by a OnceHub Administrator.

☐ Account lockout is disabled

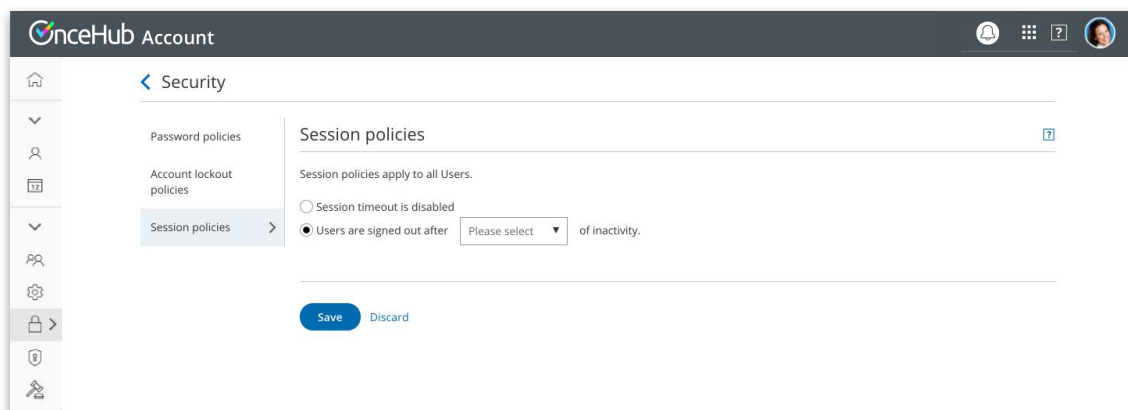
☒ Account lockout is enabled

The User is allowed  unsuccessful login attempts within  minutes before the account is locked.

**Save** **Discard**

4. Click to enable Account lockout. This protects against brute force login attempts and automatically suspends account access when multiple failed login attempts have been identified. Select the number of times a user can unsuccessfully try to login within a specific time frame. When finished, press Save.
5. Click on the Session policies section (See Figure 13).

Figure 13: The Session policies section of the Security settings



6. Click to enable Short sessions. This setting will automatically sign out users after a specific period of inactivity. Define the period of time until users are signed out. When finished, press Save.






**You are all set!** You have now set up custom security policies to protect your OnceHub account.

## Accessing customer data

The principles of data protection by design and default require that controllers limit the accessibility to customer data. This is important for OnceHub accounts with multiple users. If your account has multiple users, you should limit access to your customer data by assigning user roles and permissions.

## User roles

OnceHub has two type of users: Administrators and Members.

 <b>Administrator</b>		 <b>Member</b>
 <b>Account</b>		
Personal settings	Can access all users' Personal settings	Only has access to their own Personal settings
User settings	Can view and edit all users	Has no access to User settings
Security, Privacy, and Compliance settings	Has access to all settings	Has no access to settings
 <b>ScheduleOnce</b>		
Booking pages	Can view and edit all booking pages	Can access booking pages they own or can edit
Tools	Can access and use all tools	No access
Reports	Can access reports	No access
Activity stream	Can see all activities related to all users in the account	Can only see activities related to booking pages they own or can edit
 <b>InviteOnce</b>		
Schedule	Can schedule for themselves and for other team members	Can schedule for themselves and for other team members
Setup	Can view and edit all setup settings	Can view and edit all setup settings
Activity stream	Can see all meetings related to all users in the account	Can only see meetings they scheduled or are listed as an attendee on.

It is recommended that you limit the amount of Administrators in your OnceHub account.







While OnceHub allows you to have multiple Administrators, to comply with the Data protection by design principle, we recommend you only grant the Administrator role to users who configure setup and require access to reports. Users who receive bookings, but do not need to configure scheduling scenarios, should be granted the role of Member.

## User permissions

ScheduleOnce has additional user permissions related to booking pages.

There are four access permission levels:

- Owner:** This is the person receiving the bookings made via that page. There can only be one owner for each booking page. The owner has access to all booking and customer data related to the booking page. Both Administrators and Members can be owners of booking pages.
- Editor:** Editors do not receive bookings from the page, but have almost complete access to the booking and customer data related to that booking page. Both Administrators and Members can be editors of booking pages.
- Viewer:** Viewers cannot edit a booking page, but do have access to the booking and customer data associated with the booking page. Only Administrators can have the role of a viewer.
- No access:** No access means that the booking page will not show up in the user's account at all and the user will have no access to the booking or customer data related to the page. Only members can be assigned no access to booking pages.

	<b>Owner</b>   Admin Member	<b>Editor</b>   Admin Member	<b>Viewer</b>  Admin	<b>No Access</b>  Member
Receives bookings from the booking page	✓			
Has access to booking and customer data	✓	✓	✓	

OnceHub recommends that you only grant users permission to booking pages they require.

By assigning users roles and permissions, you can limit who has access to data related to ScheduleOnce bookings. This will allow you to ensure that you are compliant with the GDPR principles of data protection by design and default. [Learn more about user management](#)

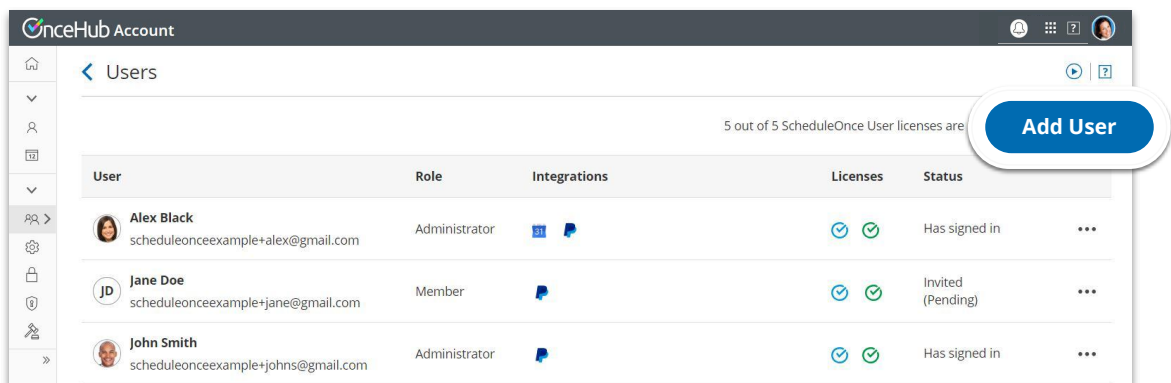
## Steps to define roles and permissions for OnceHub users

You can assign user roles when you create a new user. You can also edit an existing user's role and permissions at any time. Follow these steps to assign and edit users' roles and permissions.

### Assigning roles when creating a new user

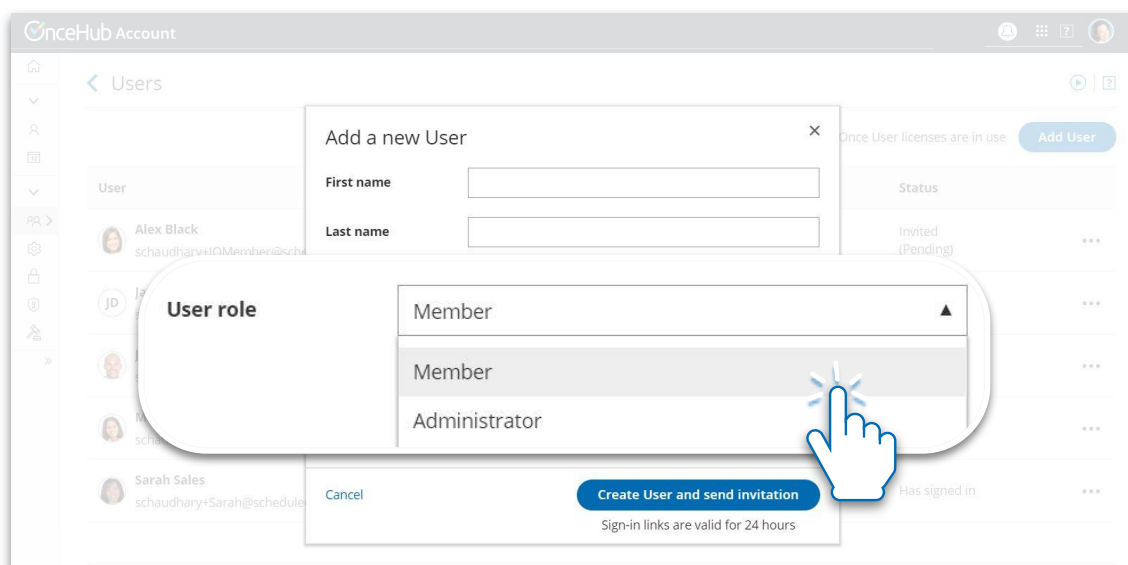
1. In your OnceHub account, go to **Account > Users** and click on the **Add User** button to add a new user (See Figure 14).

Figure 14: Click on Add User button



2. In the **Add a new User** popup, select **User role** (See Figure 15).

Figure 15: Select User role



**You are all set!** Once you click the **Create User and send invitation** button, your user will be created.

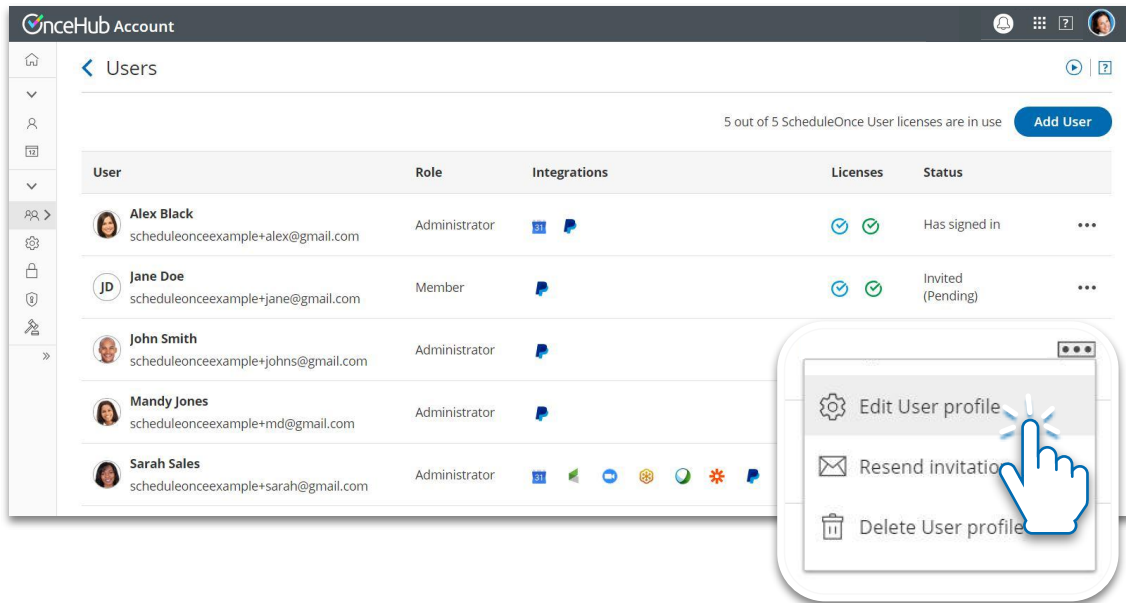


## Editing a user's role or permissions

The role and permission you assign a user can be edited at any time.

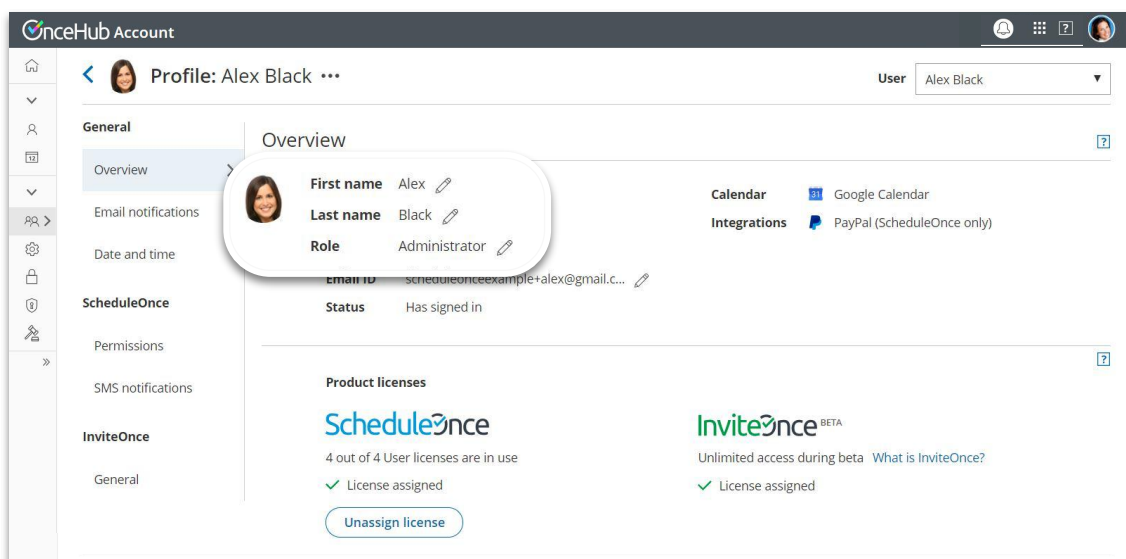
1. In your OnceHub account, go to **Account > Users** and click the **Edit User profile** from the action menu next to the user you would like to edit (See Figure 16).

Figure 16: Click on Edit User profile



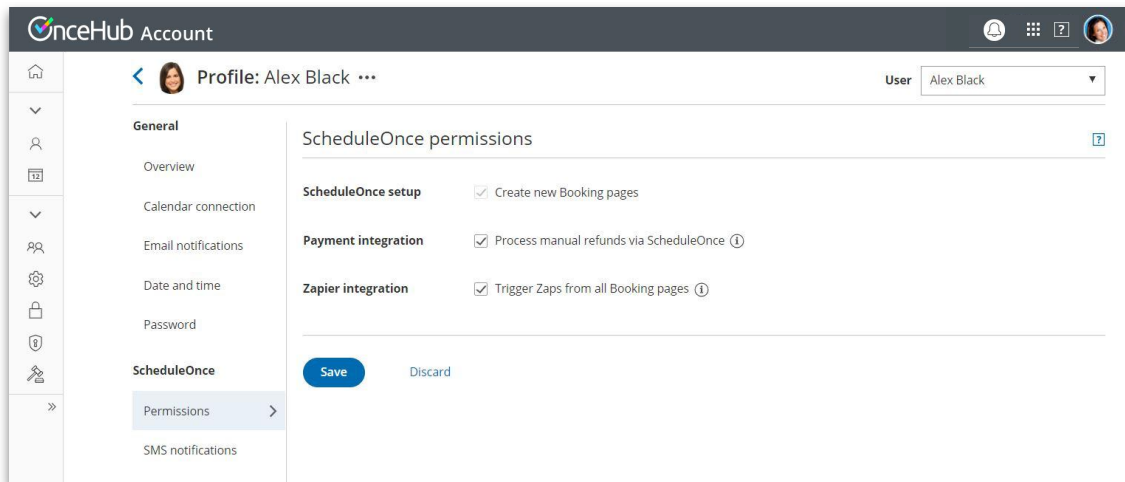
2. In the **Overview** section, you can click the pencil icon to change the Role (See Figure 17).

Figure 17: Edit User role



3. In the Permissions section, you can grant additional permissions for ScheduleOnce. There are three permissions that can be granted (See Figure 18).

Figure 18: Grant additional ScheduleOnce permissions



You are all set! Any changes made to the user's new role and permissions will take effect immediately.

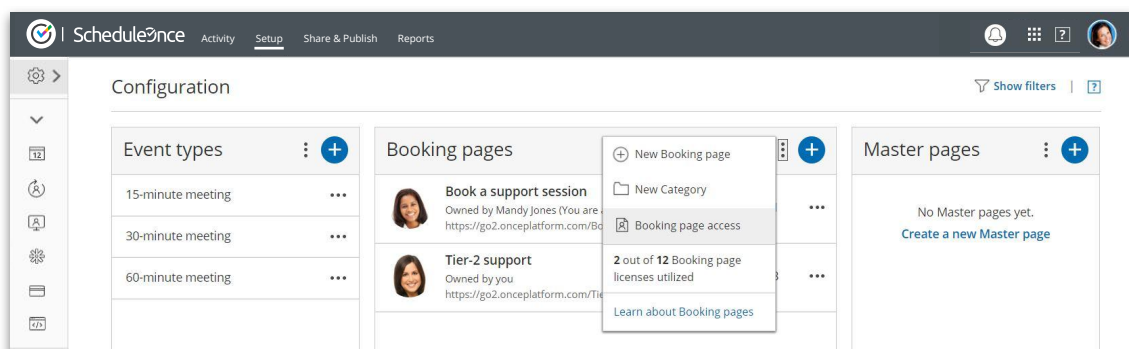
## Steps to define Booking page access permissions in ScheduleOnce

You can edit the Booking page access permissions for any users with an assigned ScheduleOnce User license. Follow these steps to edit the Booking page access permissions of a specific User.

### Editing Booking page access permissions

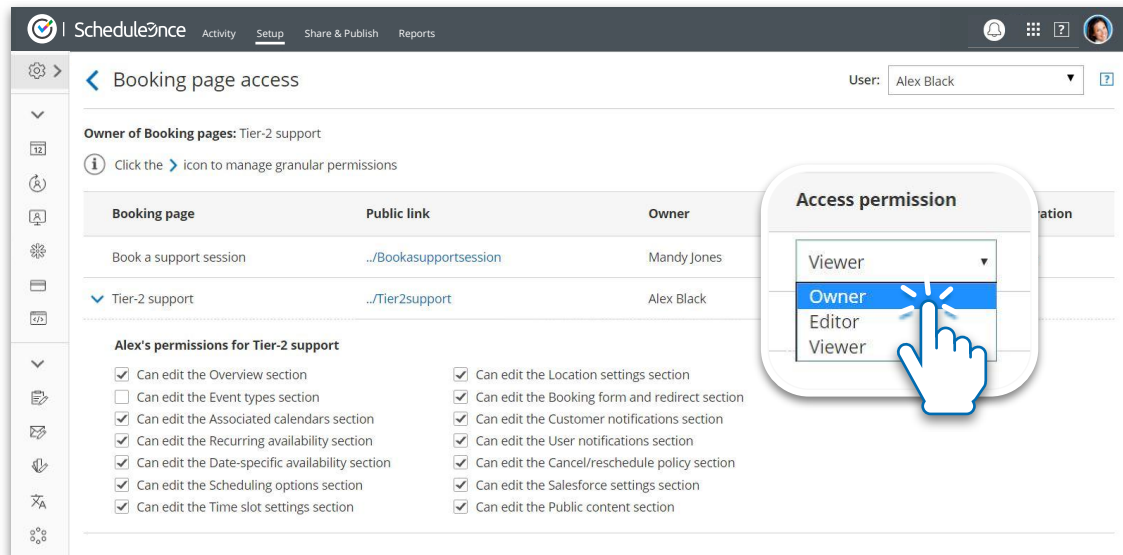
1. To edit ScheduleOnce Booking page access permissions, go to the **ScheduleOnce > Setup** page and select the **Booking page access** option from the Booking page action menu (See Figure 19).

Figure 19: Edit Booking page access permissions



2. For each User, you can edit the Booking page access permissions. When finished, press **Save** (See Figure 20).

Figure 20: Edit the Booking page access permissions



**You are all set!** You have now set up Booking page access permissions for users in ScheduleOnce.

## Data subject rights

The GDPR grants new privacy rights to data subjects. The aim of these rights is to provide transparency to individuals about how their data is being used and to give them control over the use of their own personal data ([Chapter 3](#)).

There are three rights that relate to the data you collect via OnceHub. These rights include:

- The right to access data
- The right to rectification
- The right to erasure

Controllers must be ready to comply with these rights and answer any requests from data subjects. Several of these rights may require you to access, or edit data collected via OnceHub. OnceHub provides tools to help you fulfill these rights, and is available to assist you in fulfilling any requests from data subjects. The following sections explain how to respond to certain data subject rights.



## The right to access data

Under the GDPR, data subjects have the right to know what data belonging to them is being processed by the controller ([Article 15](#)). Upon request, controllers must be able to provide data subjects with the following information:

- A report of all processed data
- Purpose of processing
- Categories of personal data
- Recipients or categories of recipients who have, or have had access to the data
- The expected period of time for which the data will be stored
- If the data was not collected from the data subject, the source of the information
- Any information regarding profiling or automated decision-making used upon the data

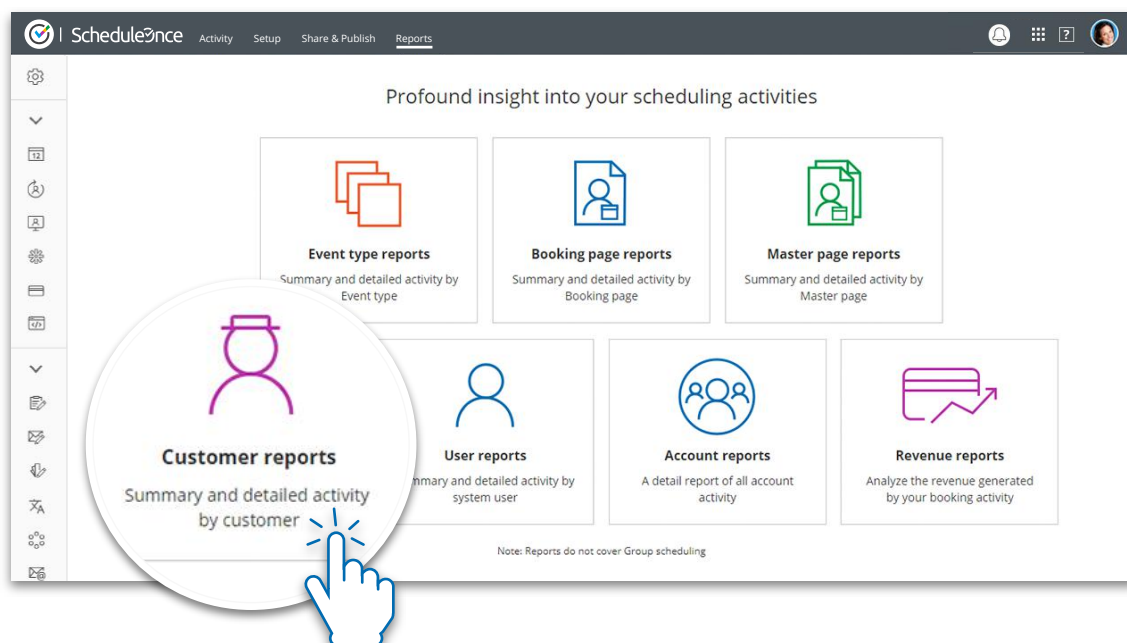
Should you receive a data access request from a data subject who scheduled with you via ScheduleOnce, you can provide a report of all data processed by ScheduleOnce by using our reports feature. If a data subject who scheduled with you via InviteOnce requests to access their data, please [contact us](#) and we will help you provide the report.

## Steps to provide data processed by ScheduleOnce

Follow these steps to generate a report for a customer who scheduled with you via ScheduleOnce.

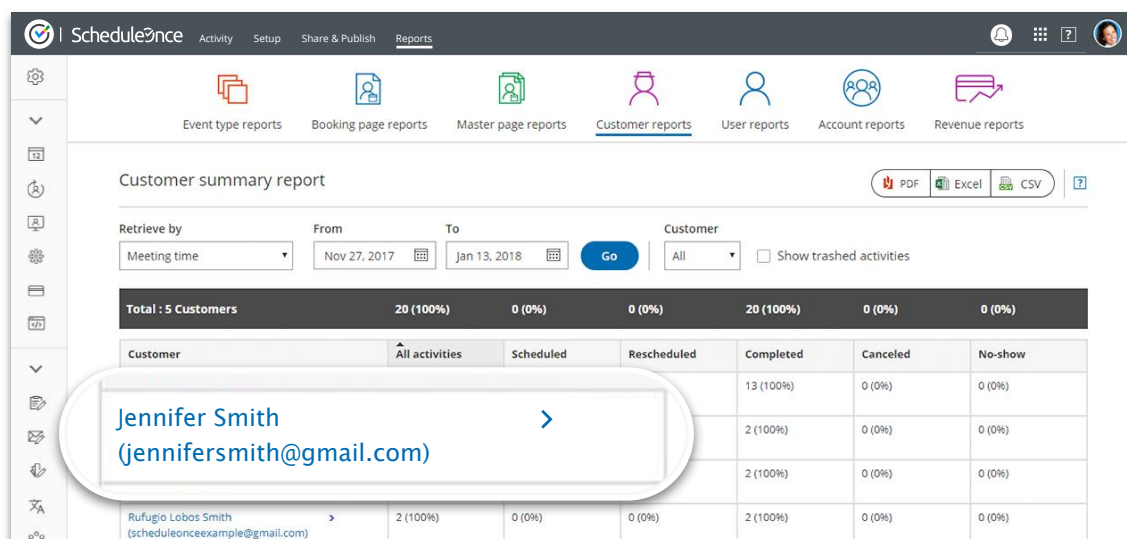
1. In ScheduleOnce, go to Reports and select Customer reports (See Figure 21).

Figure 21: Customer reports



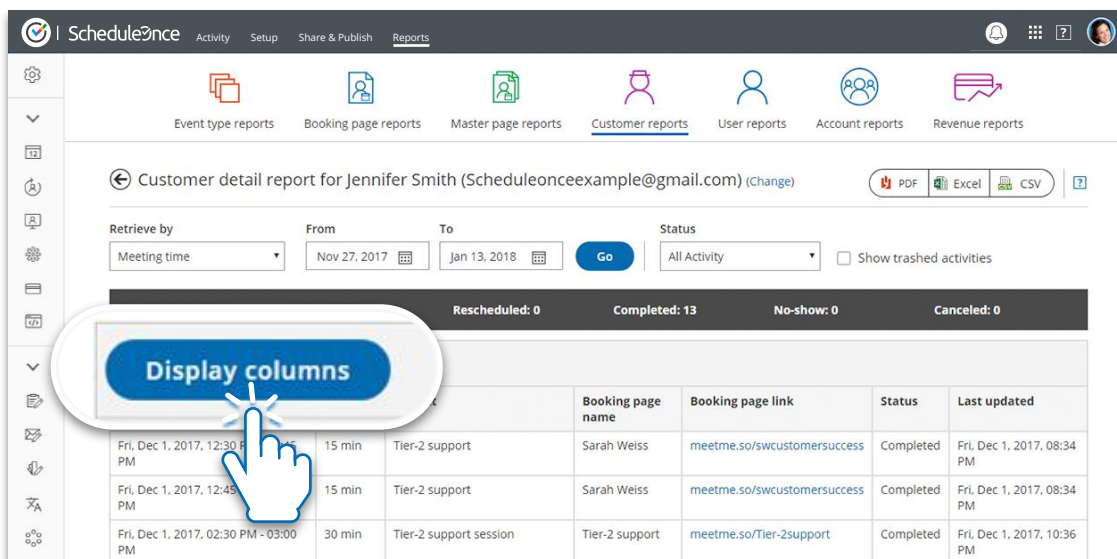
2. Select whether you want the data sorted by by Meeting time or Activity creation and select the date range of the data you want to view. To ensure you are providing a comprehensive report, your date range should start at the time you started using ScheduleOnce.
3. Next, select the specific customer to create a detailed report (See Figure 22).

Figure 22: Customer summary report



- Once you select the customer, you will see a detail report of all the customer's booking activity. You can click the **Display columns** button to add any field that you use in your booking forms to the report (See Figure 23).

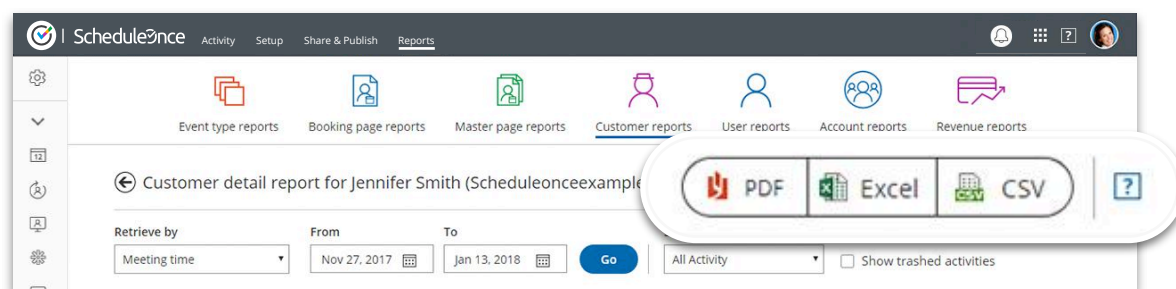
Figure 23: Customer detail report



Booking page name	Booking page link	Status	Last updated
Fri, Dec 1, 2017, 12:30 PM - 12:45 PM	Tier-2 support	Completed	Fri, Dec 1, 2017, 08:34 PM
Fri, Dec 1, 2017, 12:45 PM - 1:00 PM	Tier-2 support	Completed	Fri, Dec 1, 2017, 08:34 PM
Fri, Dec 1, 2017, 02:30 PM - 03:00 PM	Tier-2 support session	Completed	Fri, Dec 1, 2017, 10:36 PM

- When you have finished defining, you can export the report in order to provide it to your customers. You can export the report to a PDF, Excel, or CSV file (See Figure 24).

Figure 24: Export the report



**You are all set!** You have now created a report that you can share with a data subject.

[Learn more about ScheduleOnce reports](#)

## The right to rectification

Data subjects have the right to request that you correct any of their data that is inaccurate or incomplete ([Article 16](#)). Should a data subject exercise their right to rectification, [contact OnceHub](#) and we will correct the data as soon as reasonably possible.



## The right to erasure

Data subjects may request that their data be erased or deleted ([Article 17](#)). Controllers must comply with this request as long as the data is no longer required for the purpose for which it was collected. Should a data subject exercise their right to erasure, [contact OnceHub](#) and we will delete the data as soon as reasonably possible.

# Data protection impact assessments and breach notifications

OnceHub recommends that you conduct ongoing impact assessments on data collection and processing activities. Assessments should be done on a periodical basis, and whenever changes are made to any data-related processes. You can follow this guide to assess your use of OnceHub's products under the GDPR.

OnceHub provides you with materials and insights to help you conduct your assessments regarding the use of OnceHub as a processor of your customers' data. You can access our [Trust center](#) and [Legal center](#) to get insight into our controls and processes and review our legal documents. Additionally, upon request, we can provide our [SOC 2 report](#), which will give you a detailed review of our security and privacy programs.

While we do everything possible to protect customer data, the unexpected could happen. In the event of a security issue or data breach, OnceHub pledges to notify all affected parties according to the GDPR requirements. You may need to notify your data subjects if their data has been compromised.

# We are here to help!

Should you have any questions, or requests regarding your compliance with the GDPR, we would be happy to help.

**Learn more:**

Visit our [GDPR center](#)

Follow our [GDPR checklist to ensure compliance](#)

**Email us:**

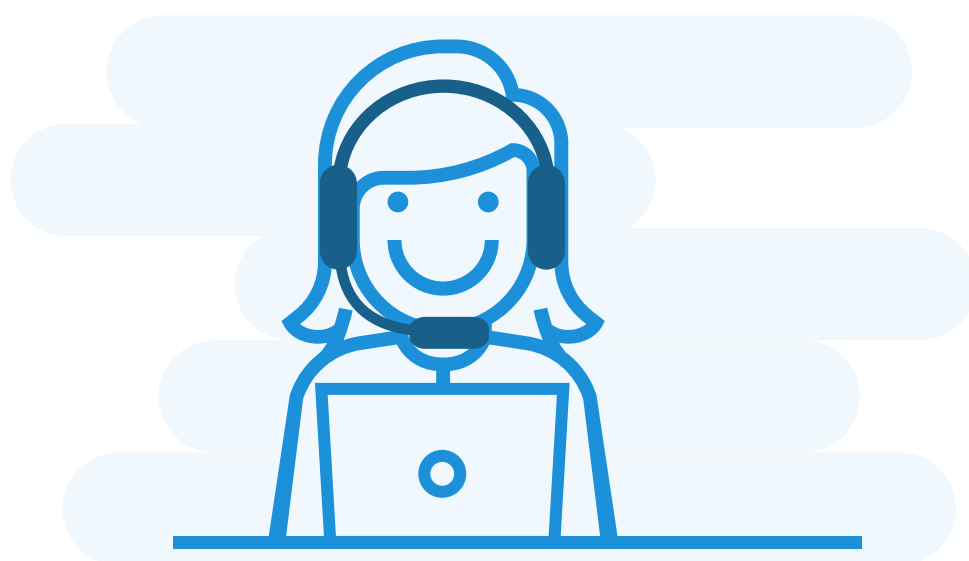
[trust@oncehub.com](mailto:trust@oncehub.com)

**Call us:**

+1.650.206.5585

US toll-free: 800.505.5257

Non-stop 24/7 support







# OnceHub

OnceHub powers organizations with smart scheduling solutions that shorten time-to-engagement in all phases of the customer lifecycle. The robust scheduling platform seamlessly integrates into existing business processes and customer touchpoints, allowing organizations to easily connect with their prospects and customers, ultimately leading to higher conversion rates and improved customer satisfaction.

To learn more, visit [www.oncehub.com](http://www.oncehub.com)

