

ScheduleOnce

A practical guide to using
ScheduleOnce in a GDPR
compliant manner



Table of Contents

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

We have created this practical guide to help you ensure your use of ScheduleOnce is compliant with the GDPR. If you are already using ScheduleOnce, 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 ScheduleOnce 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 ScheduleOnce'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



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

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

Sub-processor: Third-party businesses that perform data processing on behalf of processors. ScheduleOnce 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 ScheduleOnce.

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.

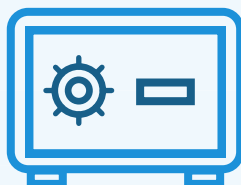
Processing: Any operation performed on personal data. This includes automated and manual operations such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating, making available, combining, restricting, erasing or destroying.

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 General Data Protection Regulation (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 ScheduleOnce users?



GDPR compliance requires commitment from both ScheduleOnce and its users. ScheduleOnce 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.

We recommend that you assess how you use ScheduleOnce to collect and store customer data and read through this guide to ensure you are protecting that data in accordance with the GDPR.

This guide covers the key requirements outlined in the GDPR that relate to the use of ScheduleOnce and 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 initiates the interaction and what data you require:

- **Inbound scheduling:** When a customer initiates scheduling by navigating to your booking page to schedule a meeting
- **Outbound scheduling:** When you initiate scheduling by sending a personalized link to a prospect or customer
- **Collection of sensitive data:** When you require sensitive data from customers during the scheduling process

Inbound scheduling

Inbound scheduling is when a prospect or customer initiates scheduling by navigating to your booking page and booking a meeting with you. 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 initiates scheduling, 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.



Outbound scheduling



Outbound scheduling is when you initiate scheduling by sending [personalized links](#) to prospects or customers. In this scenario, data is pulled from [Salesforce](#), [Infusionsoft](#), or [URL parameters](#). This means that information is processed by ScheduleOnce without any direct input 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 ScheduleOnce.

Collection of sensitive data

For organizations that process 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](#)).

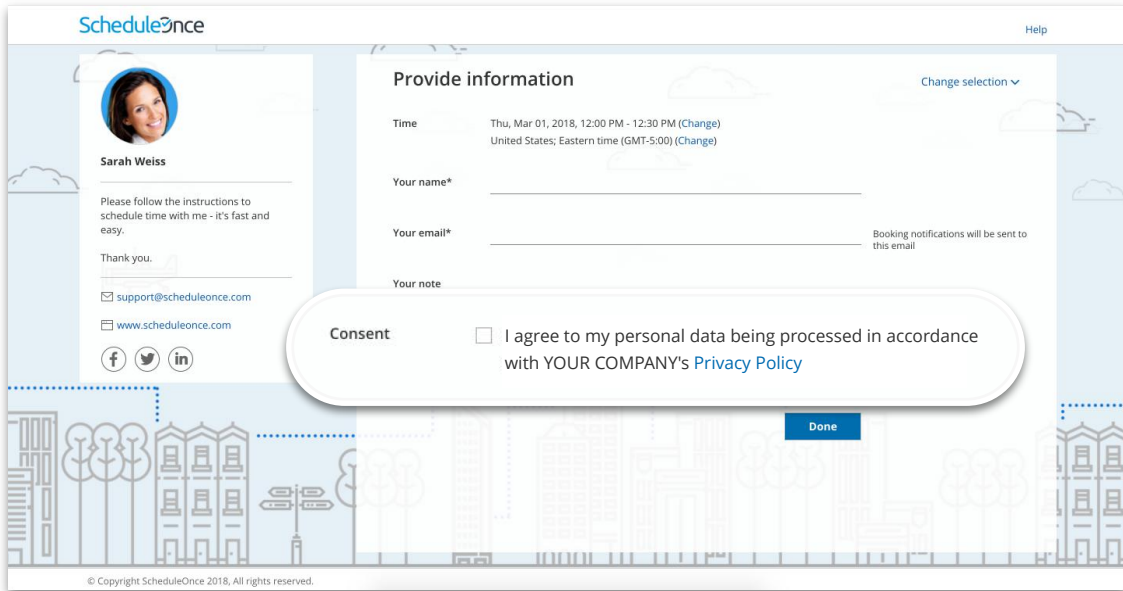


Obtaining consent for processing

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

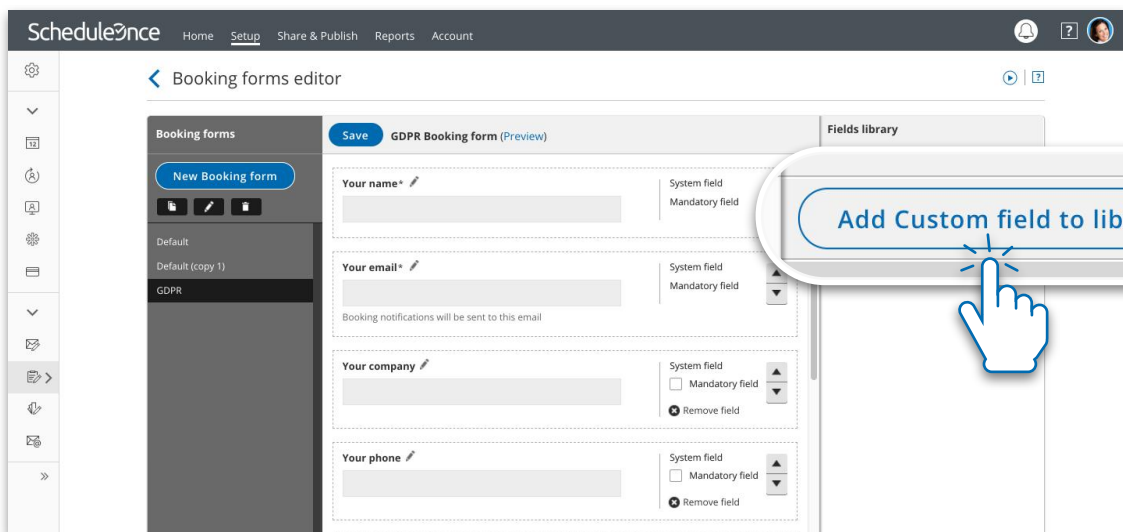
Figure 1: The Booking forms editor in the left sidebar



Setup steps

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

Figure 2: The Booking forms editor



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

The screenshot shows the 'Add Custom field to library' interface. The 'Field type' is set to 'Checkbox'. The 'Field name' is 'Consent' and the 'Field title' is also 'Consent'. Under 'Option 1', the text 'Consent in accordance with YOUR COMPANY'S Privacy Policy' is entered, with a link icon over the words 'Privacy Policy'. There are checkboxes for 'Checked by default', 'Add "Other" option', and 'Add subtext'. A '+ Add option' button is also visible.

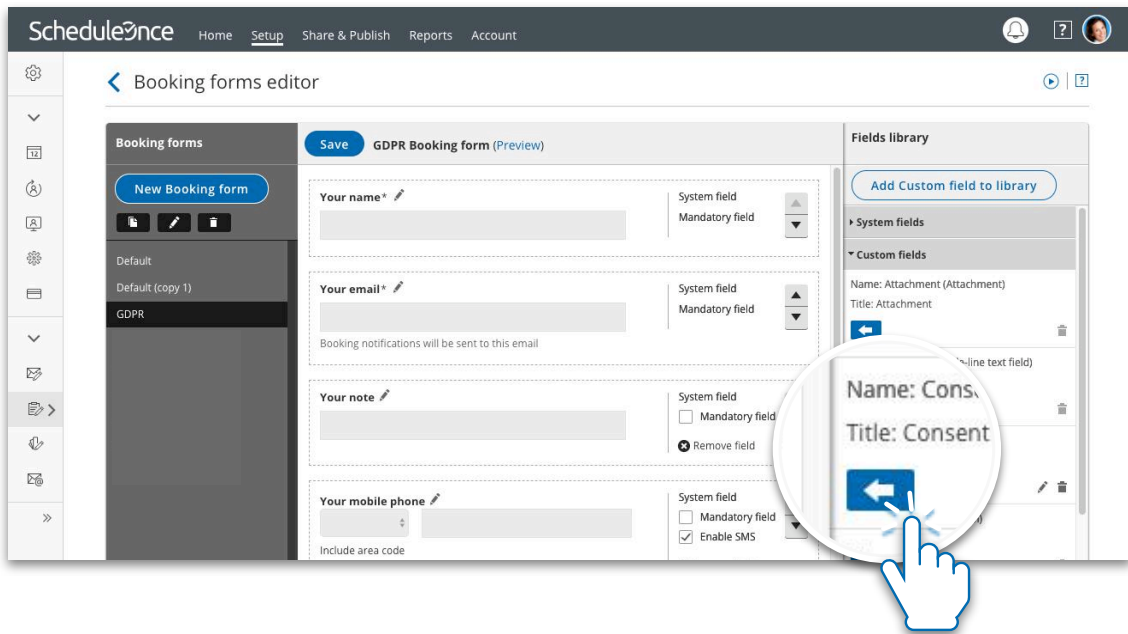
3. When creating your custom field, we recommend linking to your organization's privacy policy. This ensures your customers understand the processing activities to which they are agreeing. To link to the field, highlight the words you want to link and select the link icon (See Figure 4).

Figure 4: Link to your company's privacy policy

The screenshot is identical to Figure 3, but with a callout highlighting the link icon over the words 'Privacy Policy' in the 'Option 1' text.

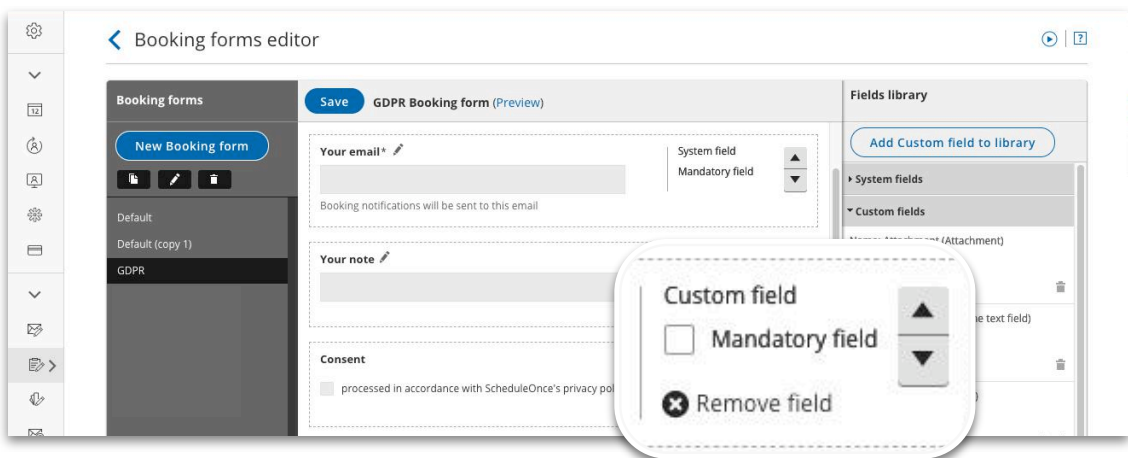
4. Input the link to your privacy policy and press save.
5. Once you have created the field, add it to your booking form by locating the field in the custom fields library and clicking the arrow to add it to the form (See Figure 5).

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 ScheduleOnce 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](#).

Additionally, if you integrate ScheduleOnce 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 ScheduleOnce 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



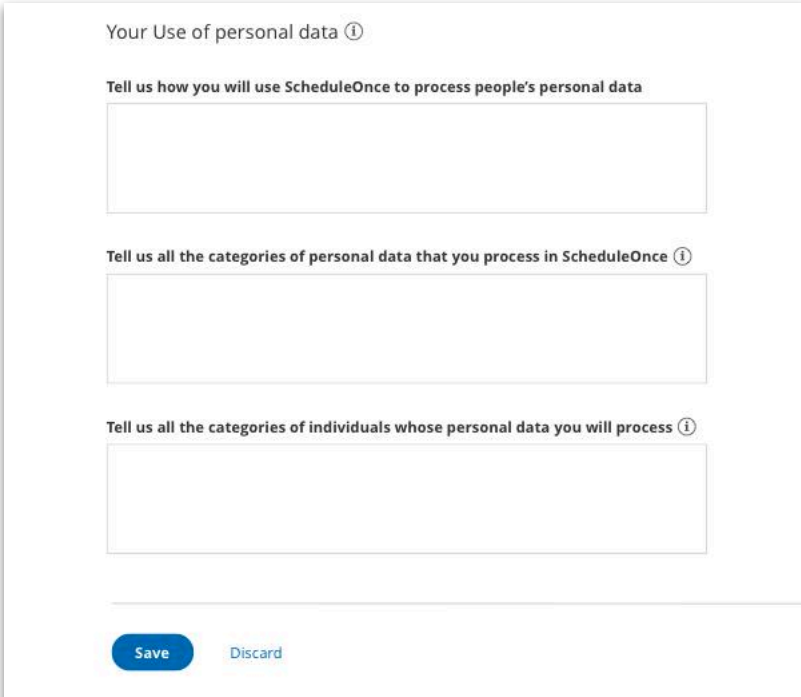
While the GDPR states that organizations with less than 250 employees may not need to keep full records of their processing activities, ScheduleOnce recommends that you maintain records to the best of your abilities.

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

Setup steps

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

Figure 7: Your use of personal data section



Your Use of personal data ⓘ

Tell us how you will use ScheduleOnce to process people's personal data

Tell us all the categories of personal data that you process in ScheduleOnce ⓘ

Tell us all the categories of individuals whose personal data you will process ⓘ

[Save](#) [Discard](#)

You're all set! You have now provided ScheduleOnce 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 ScheduleOnce need a DPO?

Using ScheduleOnce 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](#)).

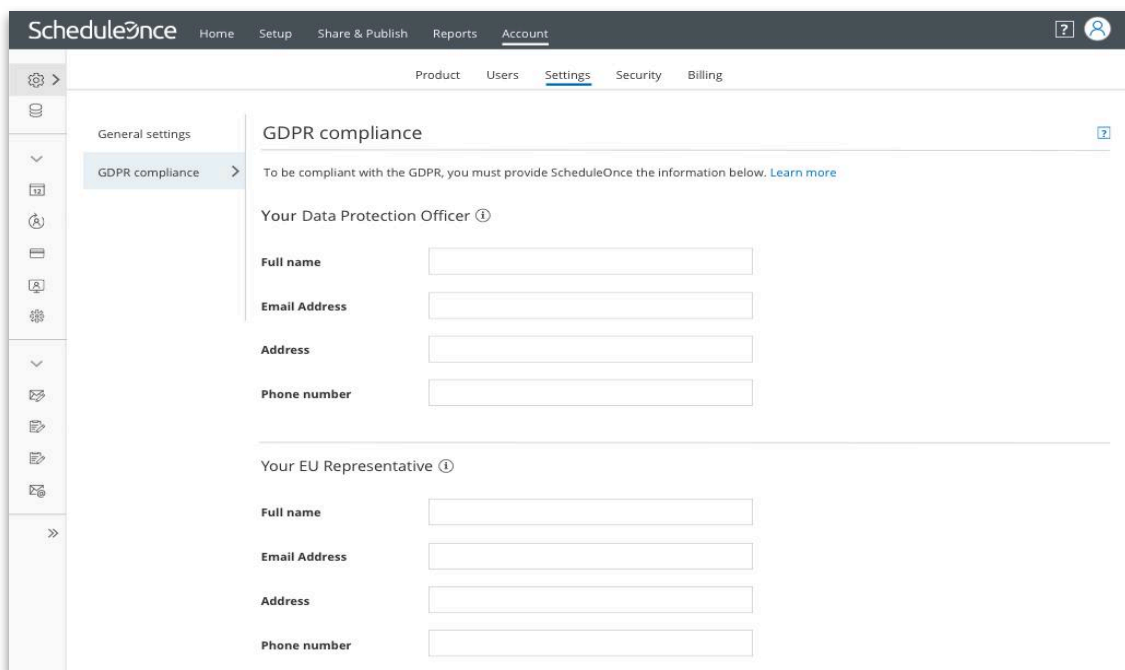
Providing contacts to ScheduleOnce

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, ScheduleOnce requires that you provide this information in your account settings.

Setup steps

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

Figure 8: GDPR compliance section of the Account settings



The screenshot shows the ScheduleOnce account settings interface. The top navigation bar includes 'Home', 'Setup', 'Share & Publish', 'Reports', and 'Account'. Below this, a secondary navigation bar has 'Product', 'Users', 'Settings', 'Security', and 'Billing'. The left sidebar contains various settings icons, with 'GDPR compliance' selected. The main content area is titled 'GDPR compliance' and includes a 'Learn more' link. It is divided into two sections: 'Your Data Protection Officer' and 'Your EU Representative'. Each section contains four input fields: 'Full name', 'Email Address', 'Address', and 'Phone number'.

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:

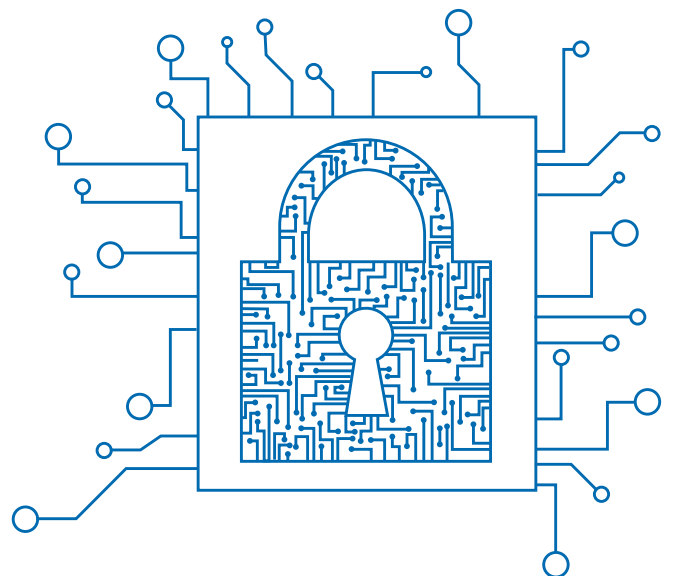
1. Data protection by design
2. Data protection by default

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 ScheduleOnce:

1. Collecting data from individuals who schedule meetings
2. Securing your ScheduleOnce 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. Data that is necessary to schedule meetings can be asked for in the booking form that individuals fill out when they schedule meetings.

What data is required to schedule a meeting?

- ◎ **Name and email address:** ScheduleOnce requires this information for scheduling a meeting. Individuals need to provide this information in order to receive a confirmation of their booking.
- ◎ **Phone number for sending SMS:** It is recommended that this field be optional, allowing individuals to decide whether or not they want to receive SMS notifications.
- ◎ **Information required for providing your service:** 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.

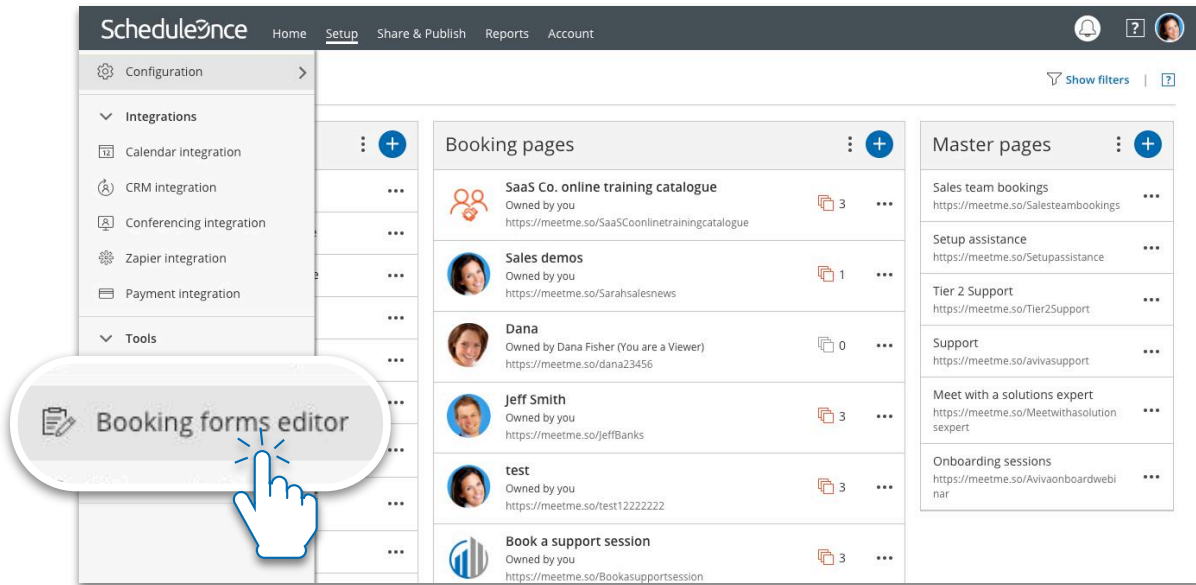
Once you have assessed what information is necessary for scheduling meetings, you can create custom booking forms to collect that information.



Setup steps

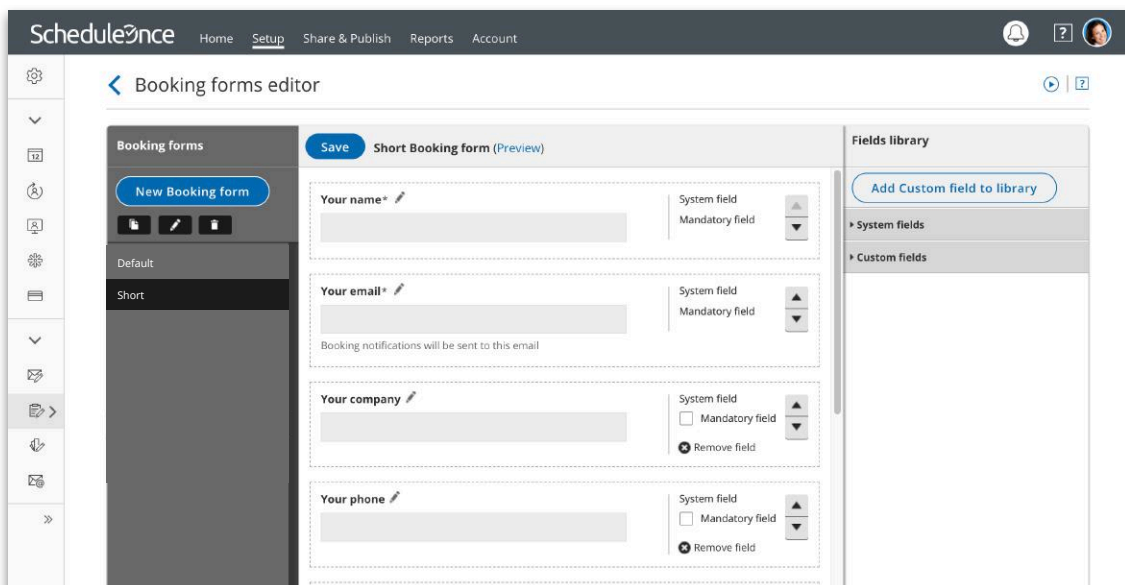
1. Go to the Booking forms editor in your account by expanding the left sidebar and selecting the Booking forms editor (See Figure 9).

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 ScheduleOnce account

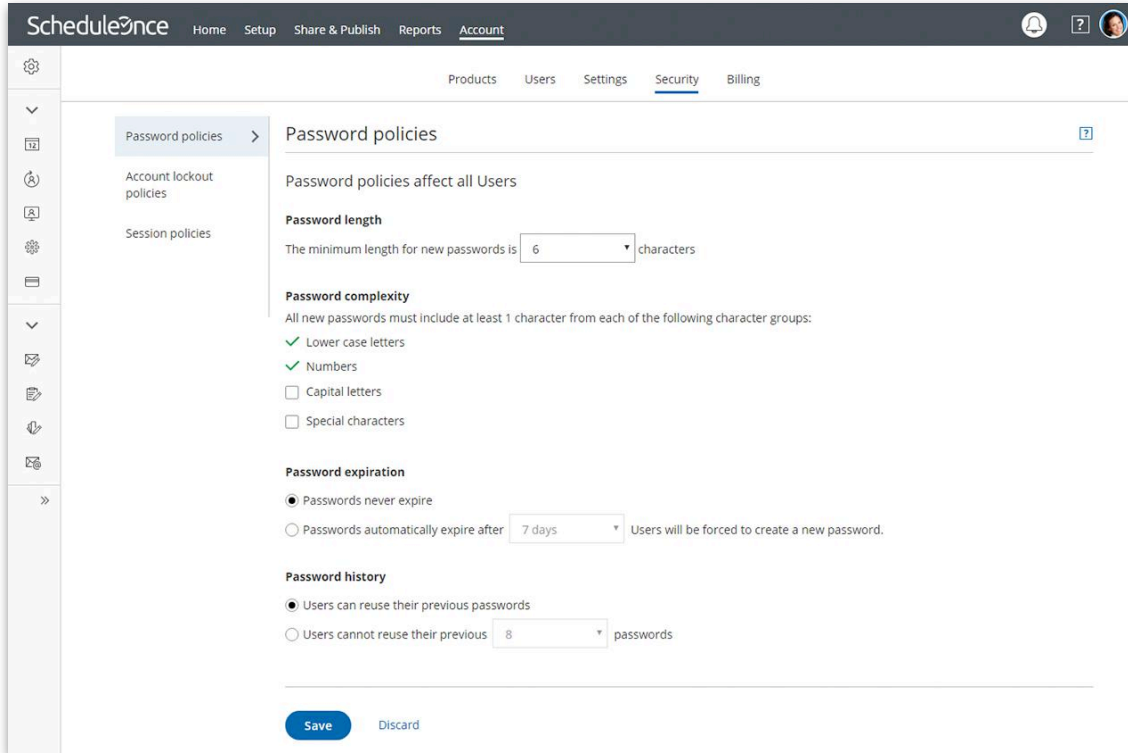
Data protection by design and default require controllers to ensure the security of their ScheduleOnce accounts. By default, ScheduleOnce requires users to use a secure password with at least six characters, including numbers and letters. In addition to our default settings, ScheduleOnce also allows 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.



Setup steps

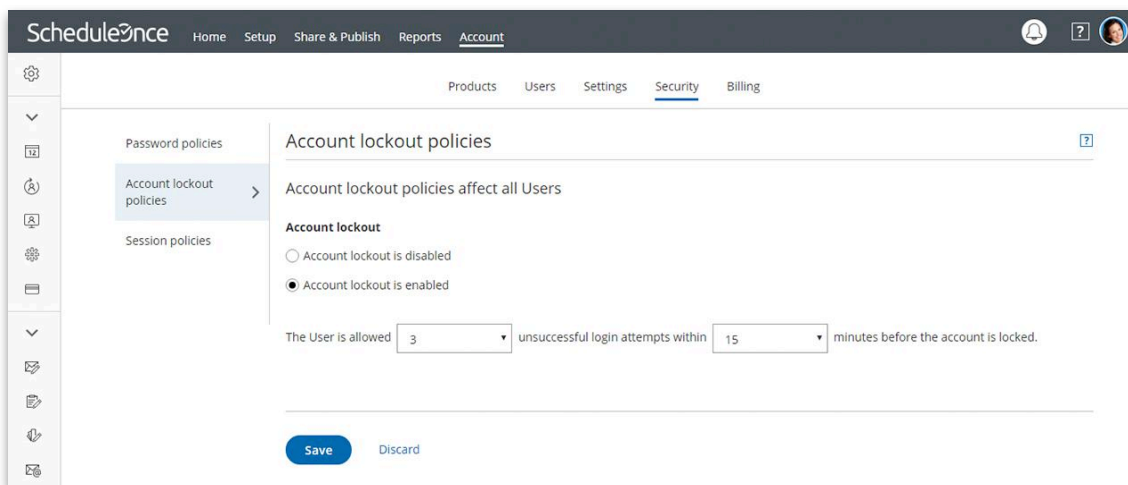
1. In your ScheduleOnce account, go to Account > Security. You will land on the Password policies section (See Figure 11).

Figure 11: The Password policies section of the Security settings



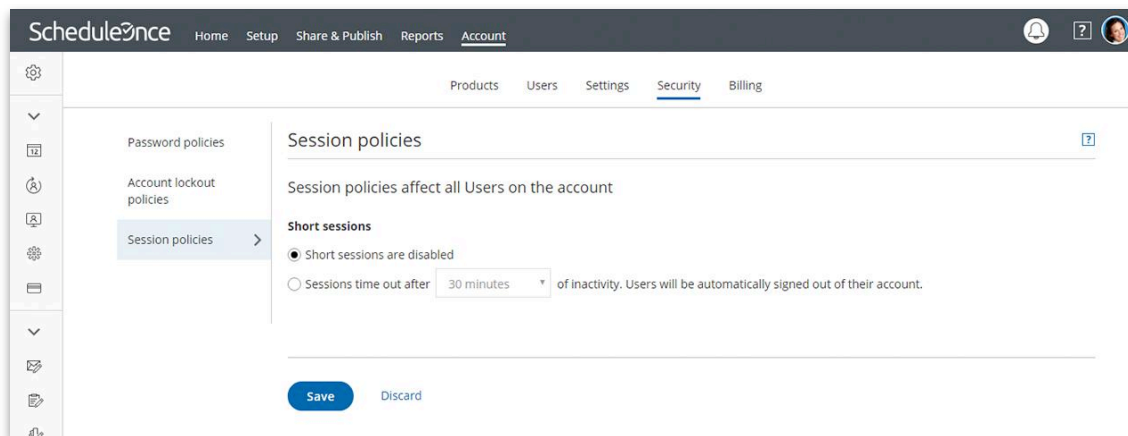
2. Define your password policy. You can set a minimum length, complexity, expiration period, and whether users can reuse their previous passwords. When finished, press Save.
3. Click on the Account lockout policies section (See Figure 12).

Figure 12: Account lockout policies section of the Security settings



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 ScheduleOnce 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 ScheduleOnce 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

ScheduleOnce has two type of users: Administrators and Members (See Figure 14).

Figure 14: The differences between Administrators and Members

	 Administrator	 Member
Booking pages	All booking pages in the account	Only booking pages they own or can edit
Booking activity	All booking activity	Only booking activity related to booking pages they own or can edit
Tools	Can access all tools	No access
Reports	Can access reports	No access

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

Aside from granting users the role of Administrator or Member, you can also grant users permissions for accessing different booking pages in your account (See Figure 15).

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.

Figure 15: Booking page permissions

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

ScheduleOnce 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 the data in your ScheduleOnce account. This will allow you to ensure that you are compliant with the GDPR principles of data protection by design and default. [Learn more about ScheduleOnce user management](#)

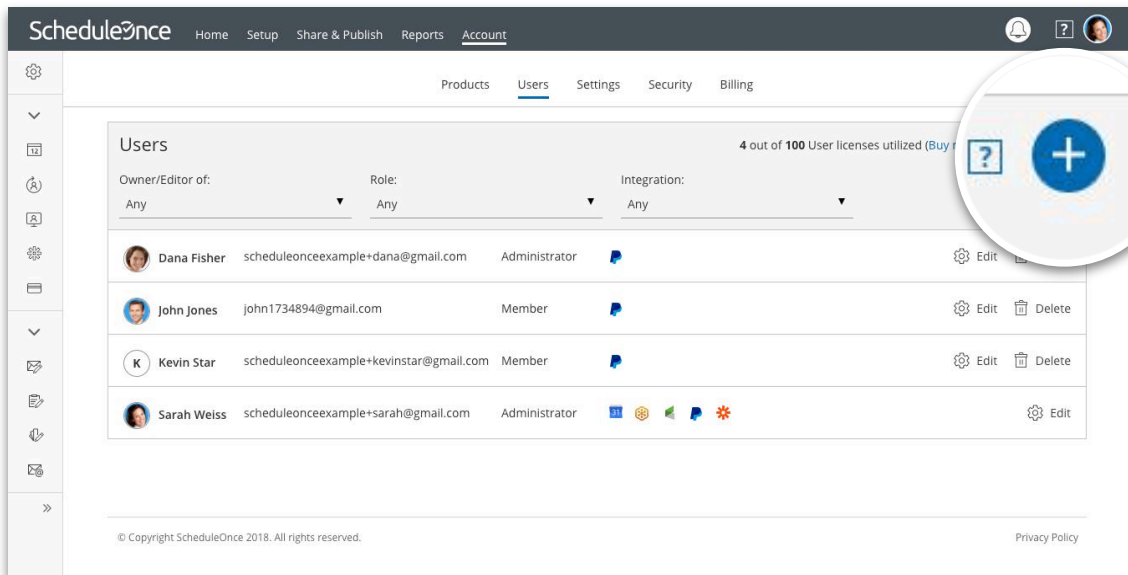
Setup steps

You can assign user roles and permissions 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 and permissions when creating a new user

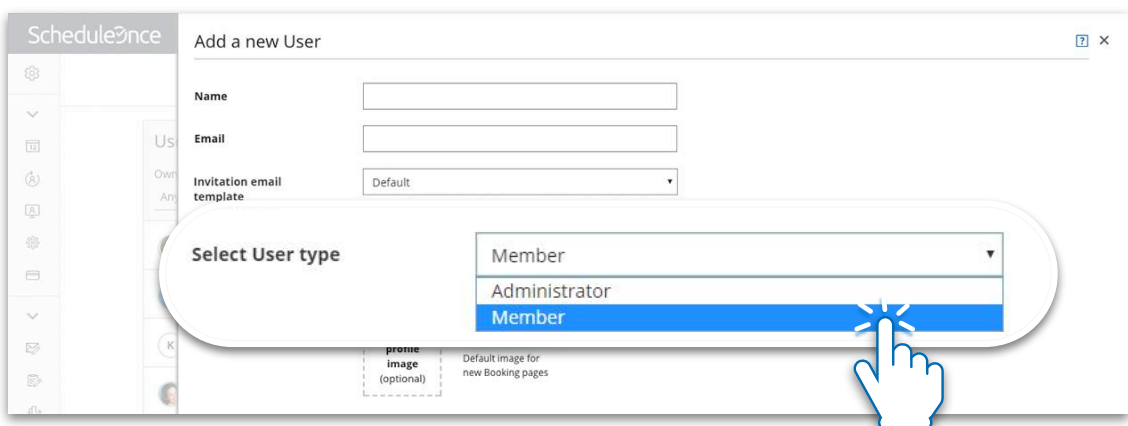
1. Go to Account > Users and click on the Plus icon to create a new user (See Figure 16).

Figure 16: The Plus icon on the Users tab



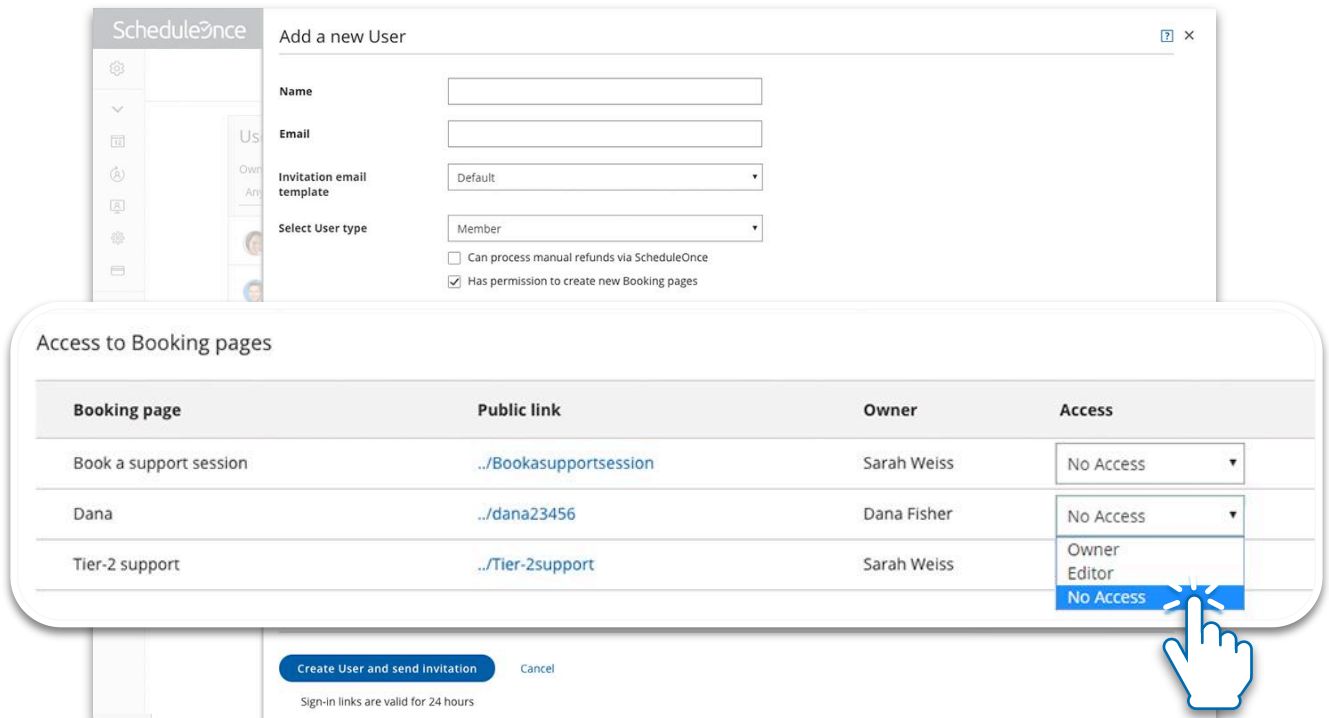
2. In the Add a new User popup, select the user type (See Figure 17).

Figure 17: Select User type in the Add a new User popup



- Next, scroll down to the **Access to Booking pages** section. Here you can determine which booking pages the user will be able to access (See Figure 18).

Figure 18: Access to Booking pages section of the Add a new user popup



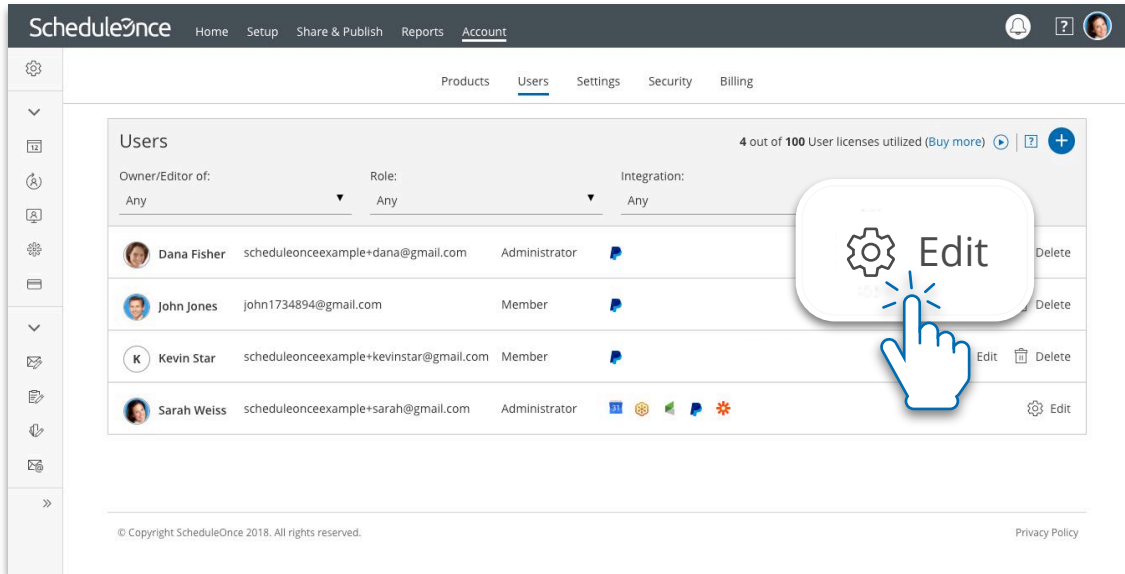
You are all set! You're all set! Once you click the **Create User and send invitation** button, your user will be created.

Editing a user's role or permissions

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

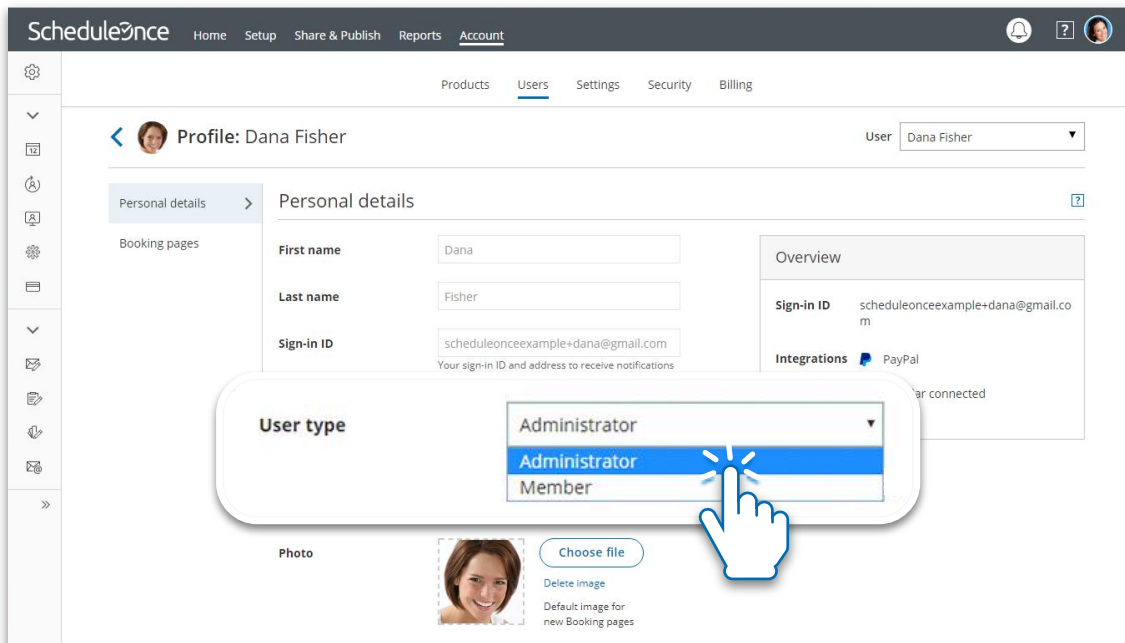
1. Go to Account > Users and click the Edit icon next to the user you would like to edit (See Figure 19).

Figure 19: The Edit icon in the Users tab



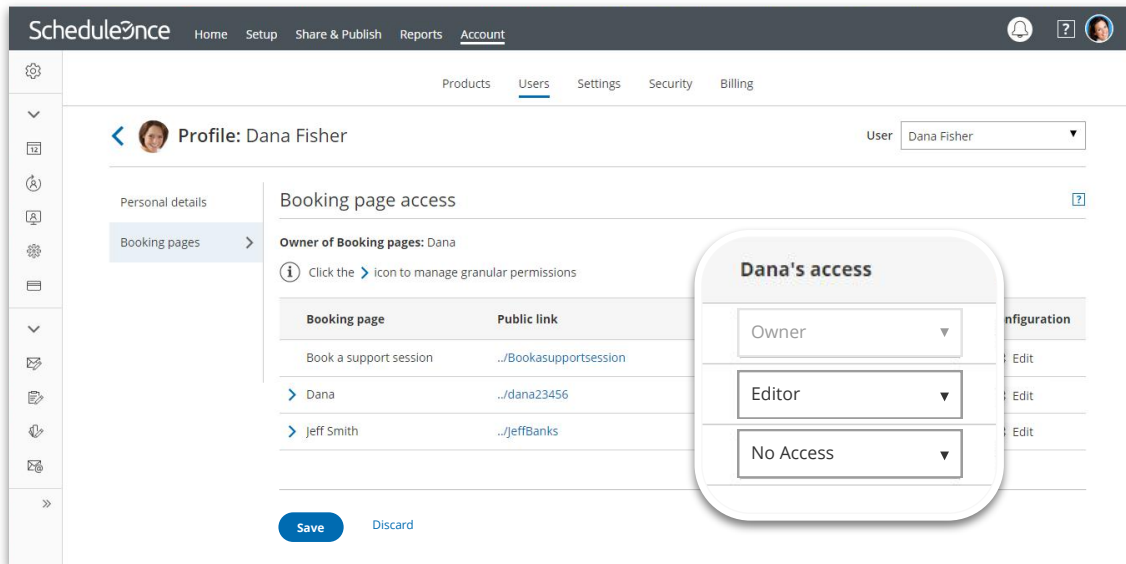
2. In the Personal details section, you can change the User type (See Figure 20).

Figure 20: Edit the User type



- To edit the user's booking page access permissions, click on the Booking pages section. Here, you can edit the user's permission per each booking page in the account (See Figure 21).

Figure 21: Edit a user's booking page access permissions



You are all set! The user's new role and permissions will take effect immediately.

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 ScheduleOnce. 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 ScheduleOnce. ScheduleOnce 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:

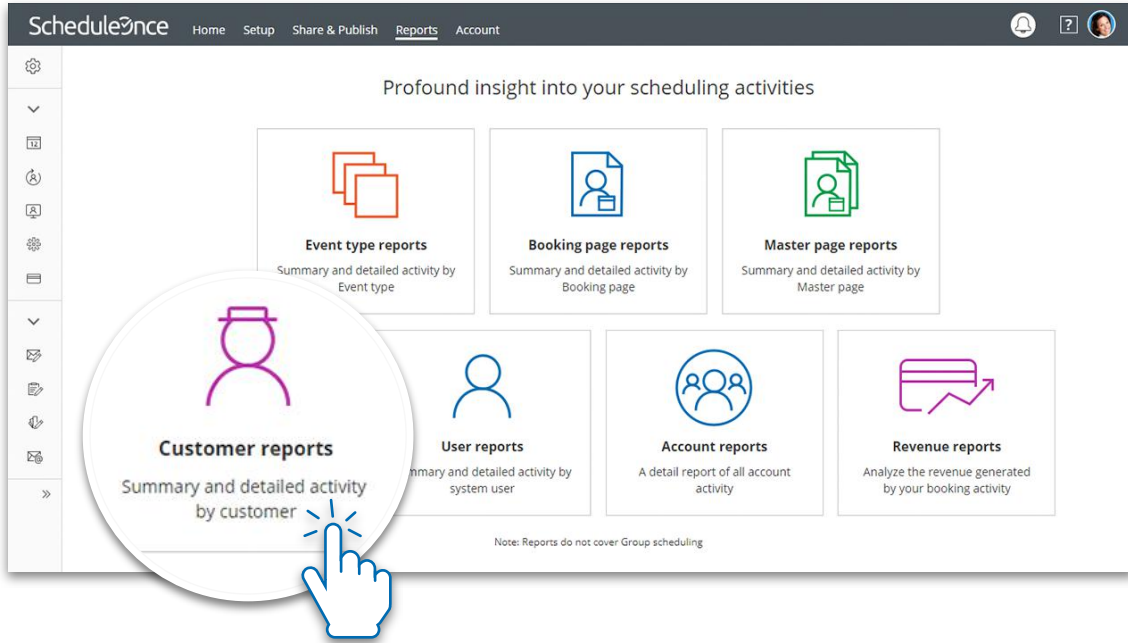
- A report of all processed data
- Purpose of processing
- Categories of personal data
- Recipients or categories of recipients who have, or have had access to the data
- The expected period of time for which the data will be stored
- If the data was not collected from the data subject, the source of 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.

Setup steps

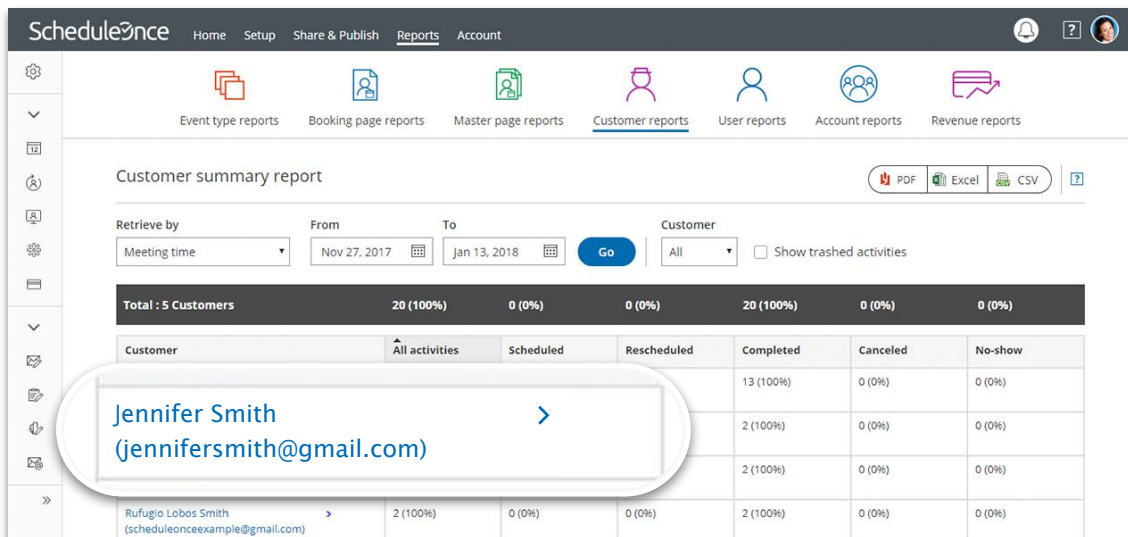
1. Go to Reports and select Customer reports (See Figure 22).

Figure 22: Customer reports



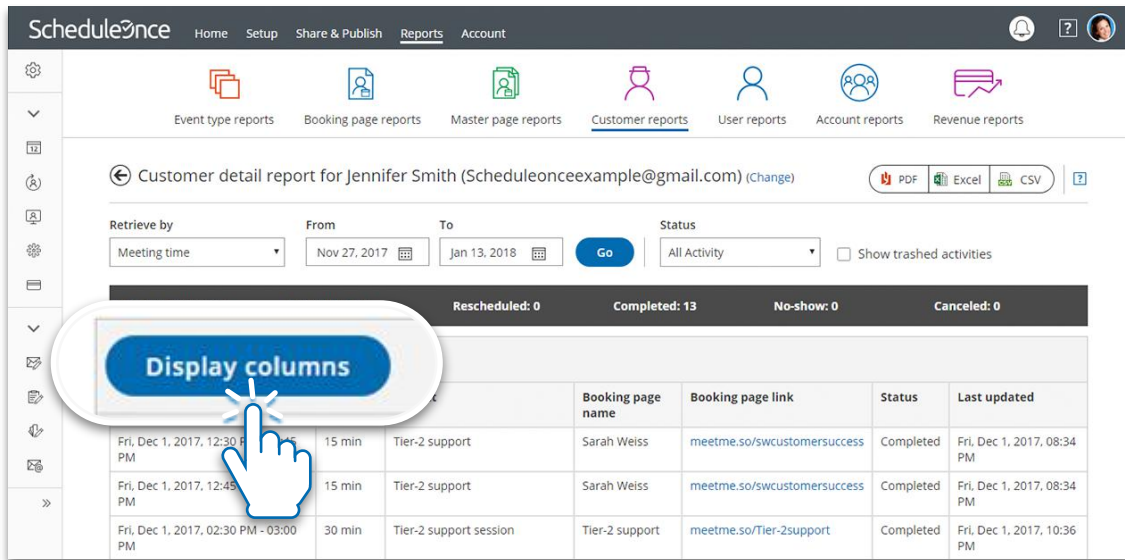
2. Select whether you want the data sorted by Meeting time or Activity creation and select the date range of the data you want to view. To ensure you are providing a comprehensive report, your date range should start at the time you started using ScheduleOnce.
3. Next, select the specific customer to create a detailed report (See Figure 23).

Figure 23: Customer summary report



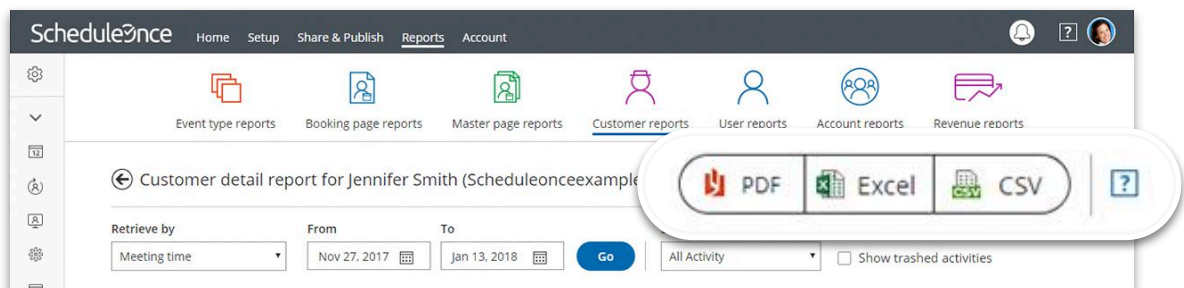
- Once you select the customer, you will see a detail report of all the customer's booking activity. You can click the **Display columns** button to add any field that you use in your booking forms to the report (See Figure 24).

Figure 24: Customer detail report



- 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 25).

Figure 25: 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 ScheduleOnce](#) 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 ScheduleOnce](#) and we will delete the data as soon as reasonably possible.

Data protection impact assessments and breach notifications

ScheduleOnce 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 ScheduleOnce under the GDPR.

ScheduleOnce provides you with materials and insights to help you conduct your assessments regarding the use of ScheduleOnce as a processor of your customers' data. You can access our [Trust center](#) and [Legal hub](#) 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, ScheduleOnce 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@scheduleonce.com



Call us:

+1.650.206.5585

US toll-free: 800.505.5257

Monday - Friday: 1AM - 9PM Eastern Time (20 hrs/day)



ScheduleOnce

ScheduleOnce is an end-to-end solution for scheduling with prospects and customers through all phases of the customer lifecycle. We connect with all major calendar platforms and provide **feature-rich integrations** with CRMs, web conferencing systems, and other online channels. Regardless of business type or industry, ScheduleOnce allows prospects and customers to professionally engage with businesses at a time that works for everyone. Our users report an up to **3x increase in conversion rates**, up to **2x acceleration in time-to-engagement**, and up to **50% time savings**.



To learn more, visit www.scheduleonce.com

