



GDPR FAQ





Contents

1. What is the GDPR and why is it important for my online presence?	3
2. When and how does this affect me as a website operator?	3
2.1 What do I need to do to avoid the pitfalls related to GDPR?	4
2.2 Will Swisscom provide me with legal support?	4
3. What do I need to do to make my website GDPR-compliant?	5
3.1 Create a privacy policy	5
3.2 Specify a legal basis for processing the data of your website users	6
3.3 Ensure that your third-party apps are GDPR-compliant	6
3.4 Find out what data your website collects	6
3.5 You should encrypt personal data	6
4. I am using the HomepageTool for my website	7
4.1 Is the HomepageTool ready for the new GDPR?	7
4.2 What functions are available to help me comply with the GDPR?	7
4.3 What additional factors do I need to consider for the HomepageTool eShop?	11



1. What is the GDPR and why is it important for my online presence?

The new General Data Protection Regulation (GDPR) came into force in the EU on 25 May 2018. It governs the protection of personal data belonging to persons who reside in the EU.

As a website owner, you are responsible for informing users of your website about how your website processes their data, particularly if they reside in the EU. It is important that you include information about how your website uses cookies and other tracking technology. According to the GDPR, you are permitted in principle to process website user data (for example, by collecting, using and storing it), but this process must meet the new GDPR requirements as of 25 May 2018. With the consent of your customers or website users, you can continue to process (that is, collect, store, manage etc.) their data within the scope of the law. You can find more information about the GDPR and its impact on Switzerland on the Swiss Confederation's official website:

- [Data protection: new European regulation](#)
- [Basic Data Protection Regulation of the European Union](#)

Switzerland is expected to follow suit in terms of privacy in the medium term (around 2020), with provisions similar to those in the GDPR taking effect nationally.

2. When and how does this affect me as a website operator?

Every operator whose website processes personal data is affected. As soon as you have website users or shop customers who reside in the EU, you are directly affected by the GDPR.

Examples of personal data:

- First name, last name
- Address
- E-Mail-address
- Date of birth
- Bank account details
- Location data
- IP-Address
- Cookie ID

The Swiss Confederation recommends using a Privacy Self-Assessment Tool, which you can access [here](#).



2.1 What do I need to do to avoid the pitfalls related to GDPR?

For companies that do not have their headquarters or a branch office in the EU, the following measures are recommended to minimize risks associated with the GDPR:

Do not acquire customers in the EU

If you sell services or products to persons in the EU, you are very likely to be subject to the GDPR. You can avoid this by restricting your customer acquisitions to the Swiss market.

To do this, we recommend you expressly state that your offer is only available to persons within Switzerland or take measures such as limiting delivery to the Swiss market or introducing geo-blocking. In addition, only offer economic goods in the languages of Switzerland and in Swiss currency (CHF), do not place an international dialling code before your phone numbers, and do not use a top-level domain (such as www.yourcompany.fr) from an EU member state.

Do not track the browsing behaviour of persons from the EU

For website users from the EU in particular, it is important that you do not track or collect their personal data without obtaining their express consent. We recommend that you refrain from using Google Analytics and other profiling tools for personalised tracking and behavioural advertising with users from the EU.

Do not use additional marketing in the EU

Do not send newsletters or other communications to persons in the EU. If you want to send newsletters and other communications, make sure you have these users' express consent and offer them the option to unsubscribe from your mailing list easily.

Your HomepageTool website is affected by the GDPR. Find out more in Section 4.

2.2 Will Swisscom provide me with legal support?

No, in principle we are not permitted to give legal advice or assistance. However, we will attempt to give you the best possible suggestions to enable you to make and keep your website GDPR-compliant.

To ensure that you are compliant with the rules, we recommend that you review the [regulation specifics](#) and seek legal advice.

For legal advice, please visit the website of the [Swiss Bar Association](#). You can find an expert near you under [Field of activity > Administrative law > Data protection law](#).



3. What do I need to do to make my website GDPR-compliant?

As a website operator, it is your responsibility to comply with the GDPR. To ensure that you are compliant with the rules, we recommend that you review the [regulation specifics](#) and consider getting legal advice (from a lawyer).

For more information on data protection and privacy, click [here](#). We offer special functions and tools for the HomepageTool that are designed to help you comply with the GDPR. Find out more below.

3.1 Create a privacy policy

A privacy policy is a statement on how data from your website users is recorded, used, forwarded and managed. Unfortunately, Swisscom cannot offer legal advice on creating your privacy policy. However, we recommend that you post a clear and comprehensive privacy policy on your website that complies with the GDPR and local privacy provisions.

Recommended content for a privacy policy

A privacy policy is a statement on how data from your website users is recorded, used, forwarded and managed. Swisscom cannot offer legal advice on creating your privacy policy because every website is different. However, We recommend that you take the following aspects into account:

- Intended purpose(s) of your data processing
- The name and contact details of the person responsible and the data protection officer
- The legal basis for data processing
- The data recipients
- How long the data will be stored
- Where appropriate, the extent to which your data is passed to third parties (including in another country or internationally).
- The right to information and/or deletion of data
- Declaration of the right to appeal with the data protection authority
- Referral to Google Analytics where appropriate

There are numerous privacy policy generators on the Internet that can help you create your own version. For small business and residential customers, we recommend the generator provided by the law firm Dr Schwenke without obligation (Link: <https://datenschutz-generator.de>) (German).



3.2 Specify a legal basis for processing the data of your website users

According to the GDPR, you are permitted to process the data of your website users (for example, by collecting, using and storing it) as long as this process meets the requirements of the GDPR. With the consent of your customers or website users, you can continue to process (that is, collect, store, manage, etc.) their data in various ways within the scope of the law.

3.3 Ensure that your third-party apps are GDPR-compliant

The GDPR makes you responsible for all third-party apps and services that are implemented on your website. Such services may include data analysis tools (such as Google Analytics, the Facebook pixel, etc.). When you review your website for GDPR compliance, ensure that these apps and services are also GDPR-compliant.

3.4 Find out what data your website collects

Every tool collects data, and some do it without your knowledge. The following questions can help you find out what data your website collects:

- What data do I collect/process/use on my website?
 - How do I collect that data?
 - Do I have a contact form? A guest book? A blog?
 - Do I use Google Analytics or another statistics tool on my site?
 - What widgets have I integrated on my site?
 - What services/products do I sell on my website?
 - Can my website be used to create products?
 - What third-party widgets and plugins have I integrated on my website?
- There are various browser add-ons that can help you, such as [Ghostery](#) and [Privacy Badger](#), which show what cookies are used on your website and all of the services you have integrated on it.

3.5 You should encrypt personal data

HTTPS for your website

As a matter of principle, personal data from your users and customers should be sent to your website using SSL encryption. We therefore recommend that you activate SSL encryption and only make your website available to users under HTTPS://. This is especially important for online orders and requests via contact forms. All of the websites hosted on the Swisscom Webhosting platform are automatically equipped with a Let's Encrypt SSL certificate. To enable HTTPS forwarding for your website, go to the [Hosting Control Panel](#) and click "Websites", then click "Edit" for the site you want and enable SSL forwarding. Please test your site's functionality after you switch to HTTPS by accessing it through the browser. In some cases you will need to take additional steps (due to mixed content, for example).

Please test your site's functionality after you switch to HTTPS. In some cases you will need to take additional steps (because of mixed content, for example).



The HomepageTool opens in HTTPS by default (you might need to republish).

TLS for your e-mail

Be sure to configure your e-mail program to use encryption when transferring login data. Use the TLS/SSL option. (You can find more information about setting up e-mail [here](#).)

4. I am using the HomepageTool for my website

The information listed below will be useful if you created your website using the HomepageTool. It lists the GDPR compliance functions available to you.

4.1 Is the HomepageTool ready for the new GDPR?

Yes, the HomepageTool offers all the necessary functions to meet the requirements of the GDPR. However, you still need to take specific steps and be familiar with certain website functions.

This is a guide giving you recommendations for preparing your website for the EU's new privacy rules. The Swisscom HomepageTool automatically collects data for you by default and anonymises user behaviour for statistical purposes. You can find more information in the cookie policy (in the general website settings under Policies).

4.2 What functions are available to help me comply with the GDPR?

Please check that you have enabled the following functions in the HomepageTool. In addition, please note that changes will not take effect until you republish your HomepageTool page (this also applies when switching to HTTPS).

Getting your users' express consent

If you wish to obtain the express consent of your website users before you process their data, you can now do so using a special HomepageTool function. This enables you to add an **opt-in function** or a **consent statement** to requests via contact forms, for instance. This function lets you define the purpose for which you wish to collect personal data and allows your website visitors to give or refuse consent. To use this feature, go to the general site settings, click the "Manage" button, then enable and define the **consent statement** (see fig. 1). Don't forget to save your changes.



Figure 1: Activation of the declaration of consent

To position the consent statement below a contact form, tick the box in the general settings for **“Display check box and consent statement for all forms on the website”** (see fig. 2).

To determine whether a customer has given their express consent, just look at their correspondence (such as e-mail, or in an encrypted CSV file). We strongly recommend that you exclude contacts who have not provided their consent from your marketing activities (such as newsletters) and remove them manually if necessary.

Figure 2: Check box Declaration of consent (example)

Did you know that your HomepageTool automatically collects data (including personal data) transferred from contact forms and makes it available to you as a CSV file? You can find this information by clicking on the contact form (Reports -> Settings) or in the respective form's settings.



Enable policies for cookies, privacy and legal notice

We strongly recommend that you enable all of the policies under the general website settings and publish them on your site.

The HomepageTool already offers you a recommendation for the [privacy policy](#) and [cookie policy](#) by default. Please note that these policies will be adjusted in future and that you may also need to adjust them on your HomepageTool website.

To do this, go to general website settings and click “Manage”. You can define your own content there for the cookie policy, privacy policy and legal notice (see fig. 3). By default, the HomepageTool already offers you a template for this purpose. As soon as you have adjusted the policies, you can integrate them in your site by ticking the boxes that read “Display on site” and “Save”.

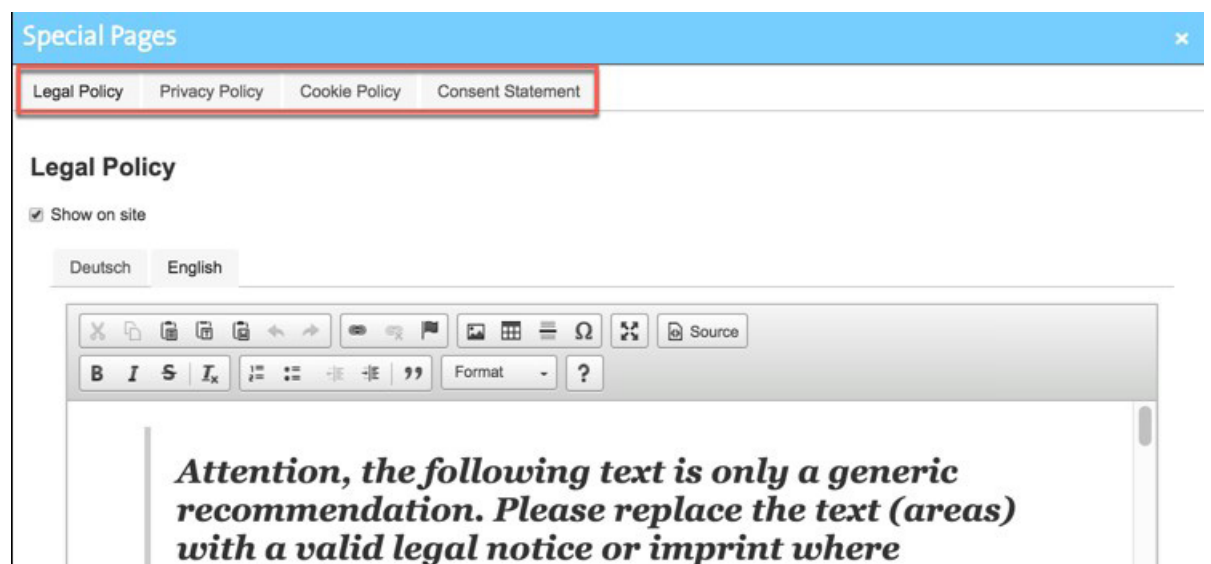


Figure 3: Policy Activation

When you enable these policies, they will typically be integrated in the footer of your HomepageTool website (at the bottom left). If this is not the case, you can try to restore the footer in the HomepageTool by clicking “Edit footer”. This will reset the footer. Don’t forget to publish your website.

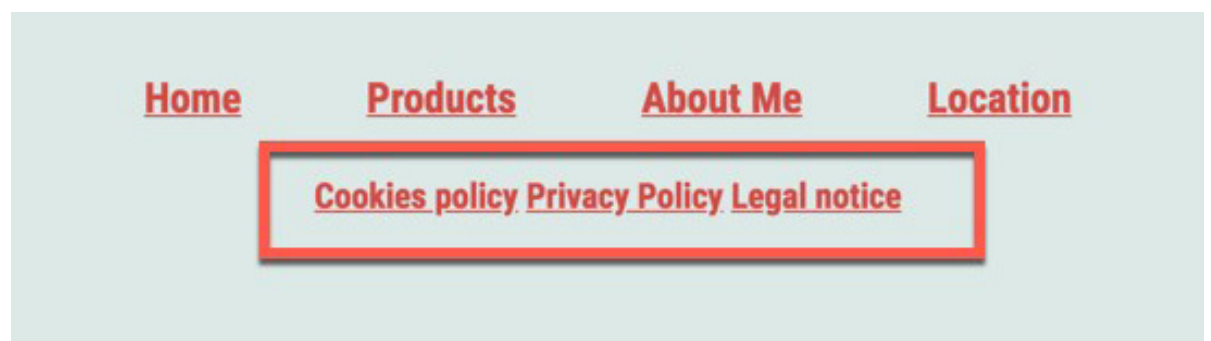


Figure 4: Activated policies in footer



Legal notice required in Switzerland since 2012

Add a legal notice to your website if you have not done so already. We have already set up a nonbinding template for you in the HomepageTool, and you can automatically transfer relevant data from the contact information (Settings -> Contact information). Be sure to double-check your details and complete or adjust them where necessary. If you need additional help creating a legal notice, we recommend you use an online legal notice generator. Click [here](#) for the legal notice generator from bag.ch(German)

Deleting personal data in the HomepageTool

a) Deleting website-form entries from CSV

If a person asks you to delete all of their records from your website, you can do so under **Settings -> Reports**. Under “Export”, just download the CSV file (see fig. 5) and manually copy the link from the “Delete Link” column so you can insert it in your browser. Open the link in your browser and you will be able to confirm that you want to permanently and irreversibly delete the information (see fig. 6). If you have multiple forms on your HomepageTool website, you may need to delete multiple records. This will guarantee that you have deleted all the personal data relating to the person in question.

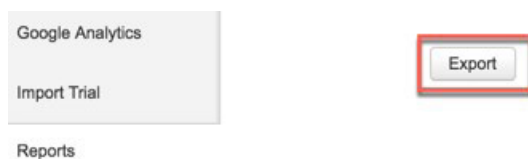


Figure 5: Export .CSV file

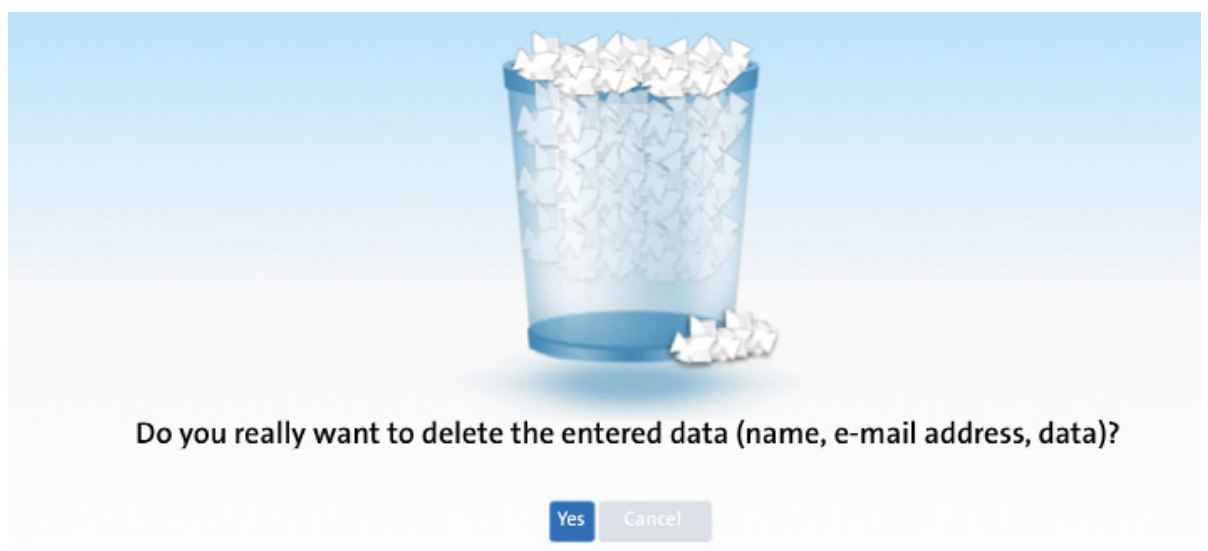


Figure 6: Final deletion of data



Don't forget that you should not include these contacts as possible recipients in subsequent marketing campaigns.

Do you need help deleting personal data in the HomepageTool? Call us on freephone number 0800 888 500.

4.3 What additional factors do I need to consider for the HomepageTool eShop?

Do you sell your services/products in the EU?

If you use the official online shop (eShop) in combination with the HomepageTool to sell your products to customers from the EU, you will need to observe the following recommendations. You will need to conclude a special processing agreement with us. Contact us about this on freephone number 0800 888 500 right away.

To ensure that you are compliant with the rules, we urgently recommend that you carefully review the [regulation specifics](#) and seek legal advice.

[Here](#) you can consult our subcontractor for information about the legal basis for processing personal data and the type of consent

You can find additional information on the GDPR and the eShop HomepageTool [here](#).

Supplementing/completing the legal information for your eShop

In addition to the mandatory legal information and policies described in section 4.2 (such as the legal notice and privacy policy), you need to provide information about GTCs, delivery costs, payments, revocation information and a revocation form. Enable these in your Administration Panel under the settings for "Legal information" (see figure 7). Once they are enabled, you can edit the respective page.

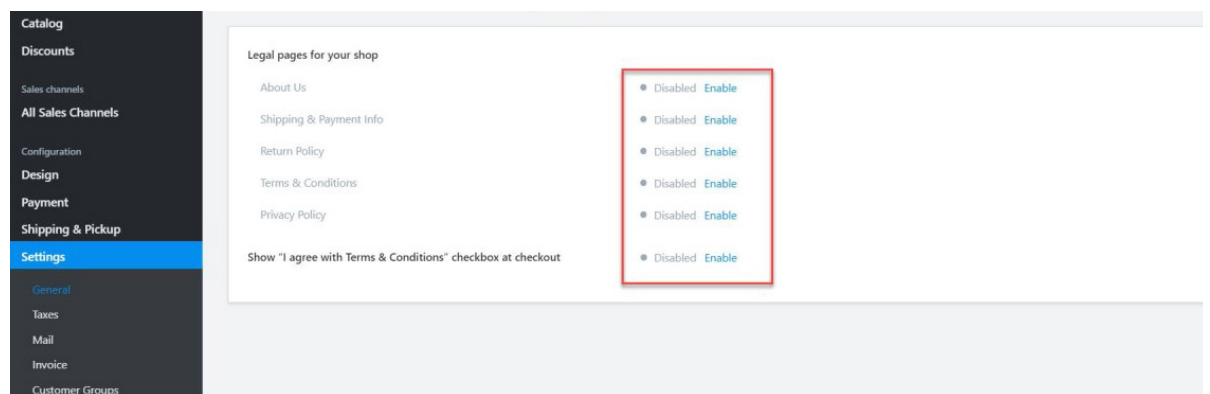


Figure 7: Activation of legal notices for eShop



We recommend that you re-enable all of the legal information for the eShop separate from section 4.2. and revise that content if necessary. Also enable the check box for users to give their consent during the payment process and define the required content.

Deleting orders in the online shop

If an EU citizen asks you to delete their personal data, you may also need to delete relevant records/data from your eShop. You will find these records in your admin area of the official webshop in the HomepageTool, not under reports as described in section 4.2. However, we still recommend that you check the reports under the general website settings as well as the eShop settings.

To do this in your HomepageTool, go to Manage Shop and click **Sales -> Orders**, then delete all of the records you need to delete.

Relevant personal data stored with third parties

If you have integrated third-party services in the HomepageTool eShop, they can independently collect personal data. Please contact the provider directly in this case.

Third-party payment providers, delivery providers and sales channels are particularly relevant here.