fccDataPrivacy for SMB and Clubs

From Order to Production Guide

Valid as of February 27th, 2020

This ***fccDataPrivacy*** From Order to Production Guide describes the process from ordering to production, the available configuration options and the installation procedure depending on the respective CMS platform.
In the first chapter it also discusses some recommendations and considerations before starting to integrate ***fccDataPrivacy*** into your website.

Table of Contents

Preface

fccDataPrivacy provides you with all the documents and tools necessary to support implementation and compliance from a data privacy point of view. However, as the owner of your website you are responsible not only for the content but also for the security of your web environment including but not limited to cyber security prevention and data security. It can be a painful experience to get hacked and personal information of your users got stolen; i.e. based on GDPR you then need to inform the supervisory authority (GDPR Art. 33 (1)) and you need to inform your users (GDPR Art. 34).

System Environment Recommendations

Keep your web environment up-to-date
It is essential to keep software systems up to date as new software releases can perform better, include new features which provide more value and – most important – provide security updates.
Please note: Be aware, that **-** based on Art. 32, GDPR - Data Protection Authorities are running online examinations of e.g. CMS systems at its own discretion to check outdated installed CMS versions, encoding, and others more[1].

Apply state-of-the-art security
Although GDPR only prescribes the encoding of webpages transferring personal data (normally forms where your visitors have to enter their personal or payment data), we strongly recommend encoding your entire website (HTTPS). Today HTTPS is used more often by web users than the original non-secure HTTP, primarily to protect page authenticity on all types of websites, secure accounts, and keep user communications, identity, and web browsing private. Search engines and visitors started to treat webpages without encoding as insecure.
On top, most Web tools offer security extensions like a Web Application Firewall protecting your site against the vast majority of common attacks (e.g. Akeeba Tools to better protect Joomla! or WordPress websites).

Check your Cyber-Security status on a regular basis
Every day more than 40 new vulnerabilities are found in software products. The time between the publication of vulnerabilities and their automated use by hackers is only a few hours.
There are independent providers out there[2] keeping an eye on your externally visible IT security risks and providing recommendations on how to strengthen your Cyber-Security status.

Password strength and rules
In 2019, the United Kingdom's NCSC analyzed public databases of breached accounts to see which words, phrases and strings people used. Top of the list was 123456, appearing in more than 23 million passwords. The second-most popular string, 123456789, was not much harder to crack, while others in the top five included "qwerty", "password" and 1111111. Using these kind of passwords hackers just need a few minutes to breach an account.

Two-step authentication

[1] e.g. https://www.lda.bayern.de/de/kontrollen.html
[2] e.g. https://locaterisk.com

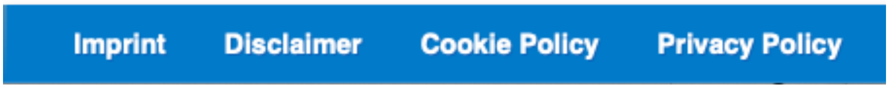
Two-step verification or two-step authentication is a method of confirming a user's claimed identity by utilizing something they know (password) and a second factor *other* than something they have or something they are (Wikipedia).
Two-step authentication - which most of you may know when doing online banking - in combination with strong password rules provides sufficient protection.

Example: https://www.fccdataprivacy.com
As an example, here's the ***fccDataPrivacy*** website security configuration:

- HTTPS encoding (SSL / TLS)
- web Application Firewall
- password complexity: min. 8 characters, must contain upper and lower characters, numbers and special character
- passwords are stored encrypted only
- two-factor-authentication (6-digit token provided by eMail or SMS)
- automated logoff after 15 minutes inactivity for administrator accounts
- no tracking Cookies
- data is stored in EU member states and Switzerland only
- regularly Cyber-Security scans.

Web Design Considerations

Before Configuration and Installation, you should have a clear view on how the Data Privacy part of your website should look like.
Visitors of your website should have direct access to the major data privacy information, independent on what page of your website they currently are (one-click access). On the market, footer menus have become established and as a result, a typical website footer could look like this:



Some comments:

- Imprint (Impressum)
  Wikipedia: An ***Impressum*** (from Latin *impressum*, "the impressed, engraved, pressed in, impression") is the term given to a legally mandated statement of the ownership and authorship of a document, which must be included in books, newspapers, magazines and websites. While there's no legal requirement for private websites to have an Imprint, an Imprint for companies and clubs must at least contain:
    - Full name and address of the site operator
    - In the case of legal entities, the full name of the company with the additional format (e.g. GmbH, GbR)
    - The written first name and surname of the person(s) authorized to represent the company or all members of the club board
    - Data for direct contact like phone number, e-mail address, fax (if available)
    - Commercial register number and register court, if available
    - Value added tax ID and economic identification number where these exist.
- Disclaimer
    - Every website operator should think about the liability for links and foreign contents on his own homepage. As a possibility for the minimization of legal risks many webmasters use a disclaimer.

It should be avoided setting a disclaimer on a website which is almost without exception considered nonsensical by lawyers. Some lawyers even assume that the author of such formulations already expects to link to legally questionable content. Then the intended exemption from liability of the site operator may turn into the opposite under certain circumstances

- There are many Disclaimer generators on the market[3] providing useful content
- there's no legal obligation to have a separated disclaimer. We've seen many websites where the Disclaimer is just part of the Imprint.

Skills Requirements

Depending on your web environment, ***fccDataPrivacy*** configuration and installation can be tricky and not all customers may have the necessary skills to deploy Java scripts correctly. If you are working with a web agency or a provider of club and agencies standard software where the web environment is integrated or you have the necessary skills in place within your organization, fine. If not, please feel free to use one of our installation partners covering your web environment.

[3] e.g. https://www.e-recht24.de/muster-disclaimer.html?mh=638ee8b2a226ac0cf624d69aac13b09163270534

From Order to Production Process

Introduction

There are some differences in the overall implementation processes for SMBs and Clubs:

- **Ease of Implementation**
  while ***fccDataPrivacy* for Clubs** is a ready-to-use pre-configured model, SMBs need customer specific processing Activities which are defined and implemented in a joint project (time & materials).
- **Payment Model**
  ***fccDataPrivacy* for Clubs** is a fully prepaid service (e.g. all payments are upfront). ***fccDataPrivacy* for SMB** has a divided payment stream, implementation and hosting fees are prepayments, creation of processing activities and other configuration support are payed as part of the joint processing activities project.

Contract

There's no explicit written contract document for the provision of the ***fccDataPrivacy*** services. All contractual terms are included in the bw-fcc GmbH General Terms and Conditions.

The major terms are:

- The contract between a customer and bw-fcc GmbH starts with the registration and payment of the initial invoice. Contract duration is 1 year and automatically extended by another year
- There's no minimal or maximal contract duration or any automatic end of a contract. A contract can end:
  - When the customer terminates in writing
  - when both parties make a joint decision to end the contract
  - bw-fcc GmbH has the right to terminate when customer is in breach of essential parts of the bw-fcc GmbH General Terms and Conditions.

Please refer to the bw-fcc GmbH General Terms and Conditions for more detailed information.

Roles & Responsibilities

fccDataPrivacy provides most of the obligations related to GDPR and the ePrivacy directive. However, some elements and actions stay in customer's responsibility.

Implementation Roles & Responsibility Overview:

Item	Comments	*fccDataPrivacy*	customer
External access to the data privacy documents	e.g. by using a footer menu on the customer website		X
Privacy Policy		X	
Cookie Policy	identifying used cookies	X	
Cookie banner		X	

Processing activities (Controller)	for SMB (joint project)
	for Clubs
		X
		X
			X

Processing activities (Processor)	for SMB
	for Clubs
		
		X
			X

Imprint and disclaimer	Impressum		X
Installation	Installation on customer’s website		X

bw-fcc GmbH or the ***fccDataPrivacy*** installation partners can support in creating the customer’s obligations.

The Overall Implementation Process

There are 5 steps to go in order to get ***fccDataPrivacy*** running:

1. Fill and submit the order form

- Select the ***fccDataPrivacy*** edition in line to your environment
- Fill the order form. The oder form is self-explaining and easy to fill (please refer to chapter **Ordering *fccDataPrivacy***).
- After submission the order is checked for correctness and consistency, an invoice is created and delivered by eMail to the eMail address specified in the ‘Customer / Club Data’ tab.

2. Payment

After payment, the following elements are created

- A customer account in the ***fccDataPrivacy*** Portal
- An administrator account as specified in the ‘Administrator’ tab of the order form. The administrator will be informed by eMail
- A default configuration for the iubenda legal documents; this includes
  - the data privacy policy in the languages requested in the order form
  - the cookie policy including the used cookies on your website (gathered using Wappalyzer, Ghostery or similar tools).

3. Configure

Customize ***fccDataPrivacy*** to best fit your environment:

- configure data privacy policy, cookie solution and cookie banner
- add additional administrators
- add users obliged to run the education lessons.

For SMB customers here’s the extra step of creating the Processing Activities (times & materials project).

4. Install

Installation of the iubenda scripts as described in chapter ***Installation Scripts.*** Please note: If you do not have the skilled resources to install by yourself, you are welcome to contact one of our installation partners.

5. Approve

The overall order process incl. installation is finished with the customer approval in the ***fccDataPrivacy*** Portal.

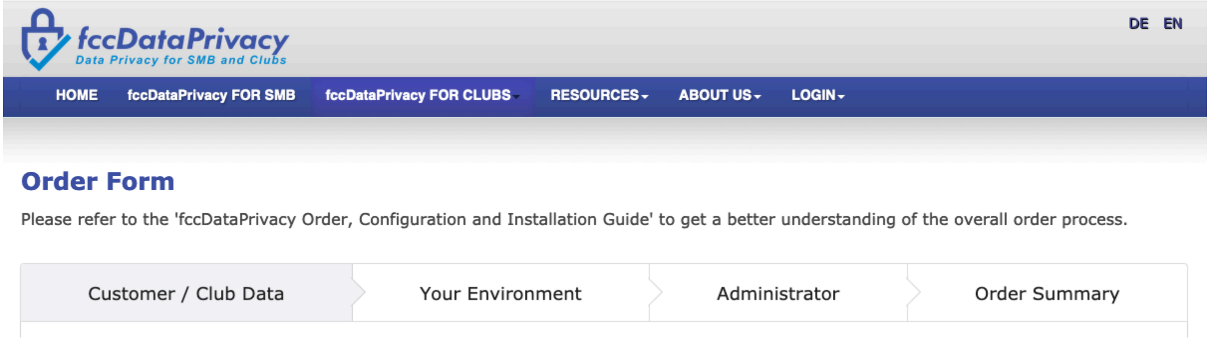
Ordering *fccDataPrivacy*

Some comments on how we handle your data:

- we strictly follow the principles relating to processing of personal data (GDPR Art. 5); i.e. we only collect data necessary to run this service (data minimization) and we keep your data for no longer than is necessary (storage limitation)
- we do not transfer your data without your consent (except when explicitly forced by law)
- we do not use any tracking cookies like Google Analytics or others.

The order form is self-explaining. The same form will appear for SMB and Club orders, only the content of some drop-down fields will show different content and some entry fields do not appear for the SMB order (as explained below).

This form is used to create a customer entry and to register the first website and the first administrator. Additional websites (in case you have more than one) can be registered within the ***fccDataPrivacy*** Admin Portal.



Order Form

Please refer to the 'fccDataPrivacy Order, Configuration and Installation Guide' to get a better understanding of the overall order process.

The Order Form is divided into 4 tabs:

- **Customer / Club data**
  - invoices are created in the language chosen when filling the order form and are sent to the eMail address provided in this tab
  - this language is also used when documents are created, e.g. processing activities, etc.

- **Your Environment**
  - please select your content management tool (CMS) your website is built with. If it isn't part of the list, enter your CMS in the next line; we then investigate how your CMS can be supported
  - please enter your website URL in the format http(s)://<your domain>, e.g. https://www.fccdataprivacy.com. We will use your website to better understand your data protection requirements
  - the next to entry fields is the product selection:
    - Select your ***fccDataPrivacy*** edition; it's all about the size of your company or club

        - Select the languages you support on your website. This is a multi-selection field, just select all languages you need
    - if you are working with a ***fccDataPrivacy*** distribution or implementation Partner, please select your partner(s)

- **Administrator**
    - This is the first administrator which will be registered for the ***fccDataPrivacy*** website and the ***fccDataPrivacy*** Admin Portal
    - After access is granted, you can add additional administrators and users in the ***fccDataPrivacy*** Admin Portal

- **Order Summary**
    - Please review your order and press the Order button
    - After submitting the order, you will receive a confirmation eMail to the eMail address specified in the Customer / Club tab.

All settings can be changed as soon as the administrator has been granted access to the ***fccDataPrivacy*** Admin Portal.

Configuration

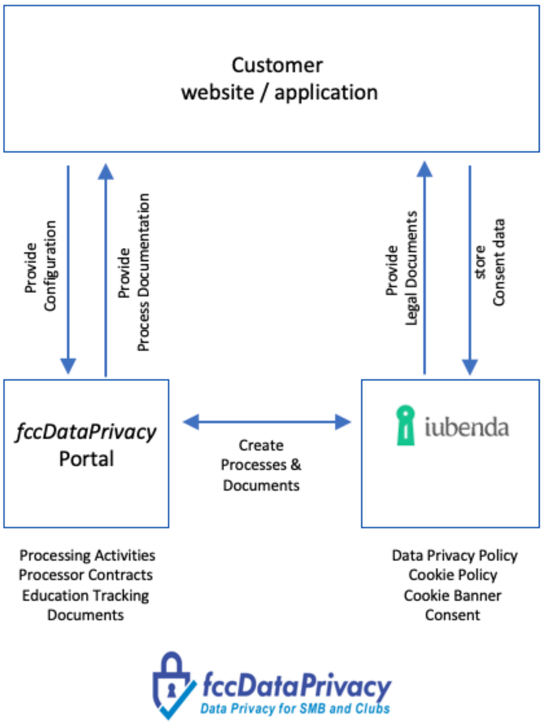
Configuration is mainly related to how the visitors of your website perceive your data protection solution.

The Systems Context

The ***fccDataPrivacy*** Portal application and iubenda together form the ***fccDataPrivacy*** for SMB and Clubs product. The iubenda service provides the Data Privacy and Cookie Policy and banner and handles the Consent while all other GDPR relevant elements are provided by the ***fccDataPrivacy*** Portal:

- Processing activities
- Processor contracts
- Data Protection Impact Assessment
- Education tracking
- Any other documents, e.g. meeting minutes.

From a customer perspective the ***fccDataPrivacy*** Portal is the visible administration and communication part, communication between the customer website and iubenda is an invisible background task.
Please refer to the ***fccDataPrivacy*** White Paper for more detailed information.



Configuration Settings

Configuration and Installation is mainly about registering the customer’s users (administrators and education users) and setting up the communication between the customer website / application and iubenda.
The configuration is entered and maintained in the Configuration section of the ***fccDataPrivacy*** Portal.

Installation

Supported Web Platforms

The way to install depends on the target web development tooling. The most common CMS systems (e.g. Jimdo, Joomla!, WordPress) provide ready-to-use plugins where the scripts can be installed just with copy & paste. With other Tools like static HTMP pages, installation may need to copy the scripts to specific places of the code.

For a current list of supported Web tools / CMS please refer to the ***fccDataPrivacy*** website (https://www.fccdataprivacy.com/en/resources/supported-platforms).

Installation Scripts

Legal documents (Privacy Policy, Cookie Policy) and Consent data are hosted by iubenda. Installation therefore means to connect from the customer website to iubenda in order to view the legal documents and get consent data stored at iubenda.
There are three iubenda connection elements to be installed:

- **Privacy and Cookie Policy**
  These legal documents (Privacy Policy, Cookie Policy) state the ways in which a website or application collects, processes, stores, shares and protects user data, the purposes for doing so and the rights of the users in that regard.

  Privacy Policy script (example)

  ```
  <a href="https://www.iubenda.com/privacy-policy/nnnnnnnnn" class="iubenda-
  white no-brand iubenda-embed iub-legal-only" title="Privacy Policy ">Privacy
  Policy</a><script type="text/javascript">(function (w,d) {var loader = function
  () {var s = d.createElement("script"), tag =
  d.getElementsByTagName("script")[0];
  s.src="https://cdn.iubenda.com/iubenda.js";
  tag.parentNode.insertBefore(s,tag);};
  if(w.addEventListener){w.addEventListener("load", loader, false);}else
  if(w.attachEvent){w.attachEvent("onload", loader);}else{w.onload =
  loader;}})(window, document);</script>
  ```

  nnnnnnnnn = unique identifier for a customer

  The Privacy and Cookie Policy scripts can be deployed as a Javascript (see above) or as an URL.

  Cookie Policy URL (example)

  ```
  https://www.iubenda.com/privacy-policy/nnnnnnnnn /cookie-policy
  ```

  nnnnnnnnn = unique identifier for a customer

  Cookie Solution
  The Cookie Solution provides the Cookie banner**.** This script needs to be installed on all pages of your website.

  Cookie Solution script (example)

  ```
  <script type="text/javascript">
  var _iub = _iub || [];
  _iub.csConfiguration =
  ```

```
{"lang":"en","siteId":1548148,"cookiePolicyInOtherWindow":true,"cookiePolicyId"
:nnnnnnnn, "banner":{
"position":"bottom","textColor":"#dadada","backgroundColor":"#5A5A5A" } };
</script><script type="text/javascript"
src="//cdn.iubenda.com/cs/iubenda_cs.js" charset="UTF-8" async> </script>
```

nnnnnnnnn = unique identifier for a customer

- **Consent**

  With GDPR, organizations need to store proof of consent so that they can demonstrate that consent was collected. These records must show:
  - When consent was provided
  - Who provided consent?
  - What their preferences were at the time of the collection
  - Which legal or privacy form they were presented at the time of the collection.

  The Consent script needs to be installed with all forms requiring consent (e.g. Account Registration, Newsletter Registration, etc.).

  Consent script (example)

```
<script type="text/javascript">var _iub = _iub || {}; _iub.cons_instructions =
_iub.cons_instructions || []; _iub.cons_instructions.push(["init", {api_key: "
mmmmmmmmm "}]);</script><script type="text/javascript"
src="https://cdn.iubenda.com/cons/iubenda_cons.js"
async></script>nnnnnnnnn = unique identifier for a customer
```

  mmmmmmmmm = unique API key for a customer

The full set of scripts is provided on a per Language basis (depending on how many document languages have been selected).

Appendix

Support

For any questions about the ***fccDataPrivacy*** Order, Configuration and Installation Guide please use the Contact Form on the ***fccDataPrivacy*** website or send an eMail to info@fccdataprivacy.com.

Trademarks

iubenda is a trademark of iubenda s.r.l, Via Torino, 2 – 20123 Milano (Italy)
fccDataPrivacy for SMB and Clubs is a bw-fcc GmbH product.

Author

Bernd Wilkens
Certified Data Protection Officer
info@fccdataprivacy.com
https://www.fccdataprivacy.com

bw-fcc GmbH
Zehntenfreistrasse 11
4103 Bottmingen
Switzerland