

Privacy Policy

In the following, we would like to inform you about the processing of your personal data in connection with the use of our website *creatingthefuture.eu*.

March 2022

Table of contents

- I. Identity and the contact details of the controller
- II. Contact details of the data protection officer
- III. Rights of the data subject
- IV. Website and log files
- V. Cookies
- VI. Contact form
- VII. Hosting
- VIII. Plugins and software

I. Identity and the contact details of the controller

The data controller responsible in accordance with the purposes of the General Data Protection Regulation (GDPR) of the European Union and other data protection regulations is:

Capital Bay Real Estate Management GmbH

Sachsendamm 4/5

10829 Berlin

Germany

Phone: +49 30 1208662 0

Email: info@capitalbay.de

www.capitalbay.de

II. Contact details of the data protection officer

The designated data protection officer is:

DataCo GmbH

Dachauer Straße 65

80335 Munich

Germany

Phone: +49 (0) 89 7400 45840

Email: datenschutz@dataguard.de

www.dataguard.de

III. Rights of the data subject

When your personal data is processed, you are a data subject within the meaning of the GDPR and have the following rights:

You have the right to

- withdraw consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal,
- obtain from the controller confirmation as to whether or not personal data concerning you are being processed, and, where that is the case, access to the personal data,
- rectification, deletion and restriction of the processing of your data,
- receive the personal data concerning you, which you have provided us in a structured, common and machine-readable format. In addition, you have the right to transfer this data to another controller without hindrance from the controller to whom the personal data was provided.

- object to the processing of your data at any time. In the event of an objection, we will no longer process your data. An exception exists if there are compelling reasons worthy of protection that outweigh your interests.

- lodge a complaint with any data protection supervisory authority, in particular in the member state of your place of residence, your place of work or the place of an alleged infringement, if you believe that the processing of data concerning you violates GDPR or other data protection law. The supervisory authority responsible for Capital Bay is the Berlin Commissioner for Data Protection and Freedom of Information.

If you have any questions about our processing of your data, please contact our Data Protection Officer.

IV. Website and log files

1. Description and scope of data processing

Every time a user accesses a domain of creatingthefuture.eu and every time a file is retrieved, data about this process is collected and used for the duration of the usage to provide content.

The following data is collected:

- Information about the browser type and the version used
- The user's operating system
- The user's Internet service provider
- Date and time of access
- Websites from which the user's system accesses our website
- Subject to your consent, information processed by Google Analytics. For additional information, please see our comments on Google Analytics.

This data is stored in our system's log files. This data is not stored together with other personal data of the user.

2. Purpose of the data processing

The storage in log files is done to ensure the functionality of the website. In addition, we use the data to optimise the website and to ensure the security of our information technology systems. These purposes also constitute our legitimate interest in the processing of your data.

3. Lawful basis for data processing

Lawful basis for the storage of your data is Art. 6 (1) (1) (f) GDPR.

4. Duration

The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected. In the case of the collection of data for the provision of the website, this is the case when the respective session has ended.

V. Cookies

1. Description and scope of data processing

Our website uses cookies. Cookies are text files that are stored within the browser or by the browser on the user's device. When a user visits a website, a cookie may be stored on the user's device. This cookie contains a characteristic string of characters that enables the browser to be uniquely identified when the website is visited again.

We use cookies to make our website more user-friendly. Some elements of our website require that your browser can be identified even after you left our website.

The following cookies may be used in the course of using our website:

1. Session cookies

- viewed_cookie_policy

2. Hotjar cookies

- _hjSession_2876963
- _hjSessionUser_2876963
- _hjIncludedInSessionSample
- _hjIncludedInPageviewSample
- _hjFirstSeen
- _hjAbsoluteSessionInProgress

3. Google (universal) analytics cookies

- _gid
- _gat_UA-221268016-1
- _gat_UA-207762995-2
- _ga

4. Webtoffee cookies

- checkbox-performance webtoffee
- checkbox-others webtoffee
- checkbox-necessary webtoffee
- checkbox-functional webtoffee
- checkbox-analytics webtoffee
- Consent webtoffee

Further information on the cookies used can be found within the explanations under VIII. plugins and software within this privacy policy.

2. purpose of data processing

The purpose of using technically necessary cookies is to simplify the use of websites for users. Some functions of our website cannot be offered without the use of cookies. For these, it is necessary that your browser is recognised even after you left our website.

Technically unnecessary cookies are used to enable us to carry out analyses in connection with the handling and use of our website. This is intended to improve our website and enhance the quality of your website visit.

3. Lawful basis for data processing

Lawful basis for the processing of personal data using technically necessary cookies is Art. 6 (1) (1) (f) GDPR.

Lawful basis for the processing of personal data using non-technically necessary cookies is your explicit and informed consent to the data processing pursuant to Art. 6 (1) (1) (f) GDPR..

4. Duration of storage, possibility of objection and elimination

Cookies are stored on your device and transmitted from it to our site. Therefore, you have full control over the use of cookies. By changing the settings in your browser, you can deactivate or restrict the transmission of cookies. Cookies that have already been stored can be deleted at any time. This can also be done automatically. If cookies are deactivated for our website, it may no longer be possible to use all the functions of the website to their full extent.

If you use a Safari browser from version 12.1, cookies are automatically deleted after seven days. This also applies to opt-out cookies, which are set to prevent tracking measures. Please send any objections to the above contact information.

VI. Contact form

1. Description and scope of data processing

Our website contains a contact form that can be used for contact. If you like to use this option, the data entered is transmitted to us and stored. The contact form and its content are processed by Capital Bay on servers of Capital Bay and within the Microsoft Office 365 environment. Due to the use of Microsoft Office 365, it cannot be excluded, that your personal data will remain within the EU or the EEA. In this respect, your personal data may be processed on servers to the United States of America, whose level of data protection has been recognised by the European Union as not providing an adequate level of data protection. In order to ensure appropriate guarantees for the protection of the transfer and processing of your personal data, which may be processed on servers in the United States of America and may thus be queried by US surveillance authorities, the data transfer to Microsoft is carried out on the basis of appropriate guarantees pursuant to Art. 46 et seq. GDPR, in particular by concluding so-called standard contractual clauses according to Art. 46 (2) (c) GDPR. A copy of the appropriate guarantees can be requested at to the contact information above.

Due to the transmission and processing of your personal data in the USA, there is the possibility that American authorities, secret services or the government gain complete access to the transmitted data. The scope, purpose and duration of this processing by the aforementioned authorities are then beyond your control. It is very likely that your rights under the GDPR will no longer be protected or that you will not be able to assert them.

The fact that this is not merely a "theoretical danger" is demonstrated by the ECJ's ruling of 16 July 2020, C-311/18.

At the time the message is sent, the following data is stored:

- o Email address
- o Name
- o First name
- o Telephone / mobile phone number
- o Company and personal information

Alternatively, it is possible to contact us via the e-mail address provided. In this case, the user's personal data transmitted with the e-mail will be stored.

The data is used exclusively for processing the conversation.

2. Purpose of data processing

The processing of the personal data from the input mask serves us solely to process the contact and answer your question. In the case of contact by e-mail, this also constitutes the necessary legitimate interest in processing the data.

The other personal data processed during the sending process serve to prevent misuse of the contact form and to ensure the security of our information technology systems.

3. Lawful Basis for data processing

Lawful Basis for the processing of data transmitted in the course of sending an e-mail is Art. 6 (1) (1) (f) GDPR. If the e-mail contact aims at the conclusion of a contract, the additional legal basis for the processing is Art. 6 (1) (1) (b) GDPR.

4. Duration of storage

The data will be deleted as soon as they are no longer required to achieve the purpose for which they were collected. For the personal data from the input mask of the contact form and those sent by e-mail, this is the case when the respective conversation has ended. The conversation is ended when the circumstances indicate that the matter in question has been conclusively clarified.

Additional personal data collected during the sending process will be deleted at the latest after a period of seven days.

5. possibility of objection and removal

If you contact us via the contact form or via e-mail, you can object to the storage of your personal data at any time. In such a case, the conversation cannot be continued. To do so, please contact us using the above-mentioned contact information. All personal data stored in the course of contacting us will be deleted in this case.

VII. Hosting

The website is hosted on servers provided by a service provider appointed by us.

Our service provider is the Dutch hosting provider, Savvii B.V. Takenhofplein 3 in Nijmegen, Netherlands. The location of the website server is geographically within the European Union.

Our website is based on WordPress with a so-called PHP programming language. WordPress is a free and open-source content management system written in PHP and coupled with a database. Features include a plugin architecture and a template system. PHP is a universal scripting language for web development.

The servers automatically collect and store information in so-called server log files, which your browser automatically transmits when you visit the website. The information stored is:

- Browser type and browser version
- Operating system used
- Referrer URL
- Host name of the accessing computer
- Date and time of the server request
- IP address

This data is not merged with other data sources. The collection of this data is based on Art. 6 (1) (1) (f) GDPR. The website operator has a legitimate interest in the technically error-free presentation and optimisation of its website - for this purpose, the server log files must be collected.

VIII. Plugins and software

We use plugins & software solutions to improve our internet presence. The plugins and tools used and how they work are explained below:

SERVICE	PROVIDER	(THIRD) COUNTRY	PURPOSE	LAWFUL BASIS	OTHER
FOR STATISTICAL PURPOSES					
STREAM	XWP.co Pty Ltd	Chelsea, Victoria (Australia)	Stream tracks the activities of logged-in users so that you can follow every change on your WordPress website in detail and clearly.	Art. 6 Abs. 1 S.1 lit. a DSGVO	https://xwp.co/privacy-policy/
HOTJAR	Hotjar Ltd.	Malta	Hotjar is a set of analytics tools that help collect qualitative data and provide	Art. 6 Abs. 1 S.1 lit. a DSGVO	https://www.hotjar.com/legal/policies/privacy/ and https://www.hotjar.com/legal/support/dpa/

			feedback through tools such as heatmaps, session recordings and surveys		
GOOGLE ANALYTICS	Google Ireland Ltd.	Ireland (USA)	Google Analytics is a free web analytics service that tracks and reports website traffic.	Art. 6 (1) (a) GDPR	https://policies.google.com/privacy?gl=DE&hl=de https://business.safety.google/gdpr/
GOOGLE TAG MANAGER	Google Ireland Ltd.	Ireland (USA)	Google Tag Manager is a tag management system (TMS) that allows you to quickly and easily update measurement codes and associated code fragments called tags on your website or mobile app.	Art. 6 (1) (a) GDPR	https://policies.google.com/privacy?gl=DE&hl=de https://business.safety.google/gdpr/
GTM4WP	Google Tag Manager for WordPress (Tamás Geiger e.v.)	Hungary	GTM4WP can insert the Google Optimize page hiding snippet so that it does not have to be manually added to a theme. This enables and improves the tag configuration and integration of Google services.	Art. 6 (1) (a) GDPR	https://gtm4wp.com/privacy
YOAST SEO	Yoast BV	Netherlands	Yoast SEO is a search engine optimisation plugin for WordPress and other platforms.	Art. 6 (1) (a) GDPR	https://yoast.com/privacy-policy/
CONTENT DELIVERY NETWORK („CDN“)					
JSDELIVR	jsDelivr is a public, open source CDN (Content Delivery Network) developed by Dmitriy Akulov and Prospect One that focuses on performance, reliability and security. It is free for everyone to use with no bandwidth limit.			Art. 6 (1) (f) GDPR	https://www.jsdelivr.com/terms/privacy-policy-jsdelivr-net
GOOGLE AJAX LIBRARIES	Google	Ireland (USA)	The AJAX Libraries API is a content distribution network and loading architecture for the open source JavaScript libraries.	Art. 6 (1) (f) GDPR	https://policies.google.com/privacy
 FONTS					
GOOGLE WEB FONTS	Google Ireland Ltd.	Ireland (USA)	Google Font is a web service that supports open source font files that you can use for web design. The integration is done locally and not via a Google API.	Art. 6 (1) (f) GDPR	https://policies.google.com/privacy
CACHE					

VARNISH	Varnish Software	Sweden	Varnish is a reverse caching proxy. As a reverse proxy, it is connected directly in front of the web server on which the website content is located. If a page request occurs, it is initially processed by the original server, but the Varnish proxy saves the request and the required content.	Art. 6 (1) (1) (f) GDPR	https://www.jsdelivr.com/terms/privacy-policy-jsdelivr-net
SOFTWARE					
MICROSOFT OFFICE 365	Microsoft Corporation	Ireland (USA)	Microsoft 365 is a subscription service from Microsoft that ensures that we always have the latest productivity tools from Microsoft. We use the Office products to carry out our work and can, for example, send you emails or create quotations.	Art. 6 (1) (1) (f) GDPR	https://privacy.microsoft.com/de-de/privacystatement
OTHERS					
WEBTOFFEE	MOZILOR LIMITED	United Kingdom	Webtoffee is a WordPress extension that we use to deploy our cookie banner.	Art. 6 (1) (1) (f) GDPR	https://www.webtoffee.com/privacy-policy/

1. Duration

Your personal information will be stored as long as it is necessary to fulfil the purposes described in this Privacy Policy or as required by law, e.g. for tax and accounting purposes.

2. Third country transfers

When using plugins and software solutions marked with third country transfer or USA, personal data may be transferred to servers in third countries outside the EU, such as the USA. The lawful basis for the processing is your consent according to Art. 6 (1) (1) (a) GDPR. The United States of America does not offer an adequate level of data protection based on a decision of the European Union. The main risk of the transfer lies in the obligation of the plugin providers to make user data accessible to American authorities under certain circumstances. A data processing agreement with standard contractual clauses is currently in place with all providers in order to make the third-country transfer as data protection-friendly and secure as possible. Adjustments to the ECJ ruling of 16.07.2020 (Schrems II, C-311/18) including additional security measures are currently being sought by us. A copy of the standard contractual clauses can be requested by sending us an informal email.

3. Notice of danger

We would like to point out that data transfer without an adequacy decision and without appropriate safeguards entails certain risks, which we would like to inform you about below:

If you consent to the use of US providers, it cannot be excluded that your personal data will remain within the EU or EEA. In this respect, your personal data may be processed on servers in the United States of America, whose level of data protection has been recognised by the European Union as not being an adequate level of data protection. Through the transmission and processing of your personal data within the US, there is the possibility that American authorities, secret services or the government gain (complete) access to the transmitted data. The scope, purpose and duration of this processing by the aforementioned authorities are then beyond your control. It is very likely that your rights under the GDPR will no longer be protected or that you will not be able to assert them.

US intelligence services use certain online identifiers (such as the IP address or unique identification numbers) as a starting point for monitoring individuals. In particular, it cannot be excluded that these intelligence services have already collected information about you, with the help of which the data transmitted here can be traced back to you.

Providers of electronic communications services headquartered in the United States are subject to surveillance by U.S. intelligence agencies pursuant to 50 U.S. Code § 1881a ("FISA 702"). Accordingly, providers of electronic communications services headquartered in the U.S. have an obligation to provide personal data to U.S. authorities pursuant to 50 U.S. Code § 1881a. Even encryption of the data at the electronic communications service provider's data centres may not provide adequate protection because an electronic communications service provider, with respect to imported data in its possession or custody or under its control, has a direct obligation to provide access to or surrender such data. This obligation may expressly extend to the cryptographic keys without which the data cannot be read.

The fact that this is not merely a "theoretical risk" is demonstrated by the ECJ's judgment of 16 July 2020, C-311/18.

4. Withdrawal and removal

You have the right to withdraw your consent under data protection law at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

You can prevent the collection as well as the processing of your personal data by the respective providers by preventing the storage of third-party cookies on your computer, using the "Do Not Track" function of a supporting browser, deactivating the execution of script code in your browser or installing a script blocker such as NoScript (<https://noscript.net/>) or Ghostery (<https://www.ghostery.com>) in your browser.