

# Privacy Policy

In force from: 5th of October 2022

## 1. Short overview

The provider of the Coconut Design Websites<sup>1</sup>, Slezsák Csilla SP is committed to the protection of personal data and the fair and transparent data processing as required by the law. Slezsák Csilla SP considers the right to self-determination in the context of data handling to be of the greatest importance for anyone involved with their business!

For this they declare the following:

- They only collect and handle personal information in accordance with the applicable law.
- They send newsletter and initiate direct contact only when explicit consent is given.<sup>2</sup>
- They notify the subjects in a timely manner using email about any changes to this policy.
- They handle personal information in a private manner and with the reasonably expectable most secure way.
- They only give personal information to 3rd parties when explicit consent is given or when required by law.
- They provide clarification to anyone about their information being processed, and anyone can request the deletion, change, handling over or locking of the information being processed about them over the contact methods provided below.

## 2. Purpose and scope of this Privacy Policy

Slezsák Csilla SP (address: HUNGARY, 2016 Leányfalu, Pusztahegyi u. 14., vat number: 55638904-1-33, hereinafter *data controller* or *controller*), as the provider of the Coconut Design Websites declares the contents of this legal document as mandatory to adhere to.

The *data controller* incurs an obligation that all *data processing* adheres to the terms of this policy as well as the regulations expressed in the applicable Hungarian and EU laws.

This *Privacy Policy* covers the following:

- *Data processing* related to the following websites (hereinafter collectively referred to as Coconut Design Websites):
  - [coconutdesign.eu](https://coconutdesign.eu)
  - [webdesignaudit.eu](https://webdesignaudit.eu)
  - [webdesignaudit.hu](https://webdesignaudit.hu)
  - [veganthemes.com](https://veganthemes.com)
- *Data processing* related to the handling and fulfilment of the orders placed in the Coconut Design Websites webshop
- *Data processing* related to the email newsletter service provided from the Coconut Design Websites
- *Data processing* related to the communication with the *data controller*

---

<sup>1</sup> For the list of domain names please refer to the next chapter.

<sup>2</sup> They may send system messages to the registered users of the website without a separate consent in justified cases.

The version of this *Privacy Policy* in force at any time can be found under the <https://coconutdesign.eu/privacy-policy/> address. The *Privacy Policy* enter into force after being published at the above address on the date stated at the beginning of the document.

The *data processor* reserves the right to change this policy at any time. If this policy is changed, the *data controller* notifies in advance all *subjects* with known contact details. Shall the *subject* find the updated terms unacceptable, they have the option to make use of their rights for example to request the deletion or the locking of their *personal data* being *processed* by the *data controller* before the updated terms would take effect. The information of those *data subjects* who cannot be notified or who do not give their *consent* to the *data processing* according to the updated policies can only be handled according to the version of the policy they accepted or in ways that do not require their *consent*. Changes that arise from the changes of the applicable law may be exempt from this restriction. In such cases the *data controller* considers a version of this policy to be in effect, that is changed in the minimum required way so that the *data processing* can be considered legal under the terms of the effective laws.

The *data controller* accepts any enquiries regarding the *data processing* at the [csilla@coconutdesign.eu](mailto:csilla@coconutdesign.eu) address.

### 3. Details of the Data Controller

Name: Slezsák Csilla sole proprietorship

Principal address: HUNGARY, 2016 Leányfalu, Pusztahegyi u. 14.

VAT number: 55638904-1-33

Email: [csilla@coconutdesign.eu](mailto:csilla@coconutdesign.eu)

### 4. Legal background

This *Privacy Policy* is made with regards to the following:

According to § 2 of the Hungarian Act CXII of 2011 on information self-determination and freedom of information (shortened and hereinafter *Info law*) the *data processing* by the *data controller* is primarily regulated by the terms of the Directive (EU) 2015/1535 of the European Parliament and of the Council (shortened and hereinafter GDPR) as a directly applicable Community measure and the applicable terms of the *Info law*.

This document is only an informal presentation of the legal framework of the *data processing* and the obligations of the *data controller*; the wording is simplified to help understanding and it only contains an excerpt of the terms applicable to the *data processing* performed by the *data controller*. With regards of the legal framework around the *data processing* the Hungarian law and the legally binding acts of the European Union shall be considered decisive. The list of these is provided at the end of this *Privacy Policy*.

Slezsák Csilla SP *processes personal data* primarily when the subject has given consent to the *processing* of his or her *personal data* for one or more specific purposes. On top of that *personal data* may be *processed* for other reasons as well, such as when the *data processing* is required for the fulfilment of a contract or lawful requirement, when it is required to protect the vital interests of

the *data subject* or of other persons or when the *data processing* is necessary for the legitimate interest of the *data controller* or a *3rd party*.

Where the *personal data* are collected from the *data subject*, the *data subject* shall be informed about the following no later than the time when the *personal data* are obtained:

- the identity and the contact details of the *data controller* and, where applicable, of the *controller's* representative;
- where applicable, the contact details of the data protection officer (none);
- the fact of the *data processing*;
- the range of persons who are *data subjects*;
- the intended purposes of the *data processing*;
- the legal basis of the *data processing*;
- the interests where *processing* is based on legitimate interests pursued by the *data controller* or by a *3rd party*;
- the list of *recipients* or categories of recipients to whom the *personal data* will be disclosed;
- the fact of the transfer of *personal data* to *third countries* or *international organisations* if any;
- the period for which the *personal data* will be stored, or if that is not possible, the criteria used to determine that period;
- the rights of the *data subjects* and their options for judicial remedy; and
- the obligations for the *data subject* to provide the *personal data* and of the consequences, where they do not provide such data.

Where the *personal data* are NOT collected from the *data subject*, the *data subject* shall be also informed about the following within a reasonable period after obtaining the *personal data*, but at the latest within one month, or at the first time contact is made with the *data subject*, or at the first time the *personal data* is transmitted to a *3rd party* or another *recipient*<sup>3</sup>:

- the categories of *personal data* being *processed*;
- the source of the *personal data* and the fact if they are sourced from a publicly accessible database

The *data controller* aims to provide the above described information directly to the *data subjects*, but in some cases providing the information in a direct manner may be impossible or may involve a disproportionately high amount of effort or it may likely interfere with the legitimate interests pursued by the *data controller*. In such cases the *data controller* shall implement suitable measures to safeguard the *data subject's* rights and freedoms and legitimate interests, including the publication of the above information in this document or in its appendix.

## 4.1. Definitions of terms and their explanation

This chapter provides an excerpt of the terms from the *Info law* and GDPR which are relevant to this document together with any other terms used with a specific meaning throughout this document.

### 4.1.1. Persons, organisations and roles:

**data subject (subject):** a natural person identified or identifiable based on any information;

---

<sup>3</sup> Latest at the time when any of the three event happens.

**user:** a natural person, who becomes a *data subject* in the context of the information technology services provided by the *data controller* or the *data processors*;

**data controller (controller):** the natural or legal person or organisation which determines the purposes and means of the processing of *personal data* and performs the *data processing* or orders a *data processor* to perform it – Slezsák Csilla SP in the context of this document;

**data processor (processor):** the natural or legal person or organisation which processes *personal data* as commissioned or ordered by the *data controller*;

**recipient:** a natural or legal person or organisation from whom the *data controller* or the *data processor* discloses *personal data*, regardless if it is a *3rd party* or not (so for example the *data processor* is a recipient too);

**3rd party<sup>4</sup>:** a natural or legal person or organisation other than the *data subject*, *data controller*, *data processor* and persons who, under the direct authority of the *data controller* or *data processor*, are authorised to or do perform the processing of *personal data*;

#### 4.1.2. Data

**personal data:** any information regarding the *data subject* – including conclusions inferred from other information;

**sensitive data:** any *personal data* which falls under the special categories of *personal data*, for example information regarding religious or philosophical beliefs

#### 4.1.3. Operations performed on or with data

**data processing:** any operation or set of operations which is performed on *personal data* or on sets of *personal data*, regardless of the methods used, especially the **collection**, recording, **organisation**, structuring, **storage**, adaptation or alteration, retrieval, consultation, use, **disclosure by transmission, dissemination or otherwise making available**, alignment or combination, **locking, erasure or destruction**, also the prevention of further use, making a photo, an audio- or a video-recording or any other recording of physical attributes capable to identify a person;

**restriction of processing:** the marking of stored *personal data* with the aim of limiting their *processing* in the future (e.g. locking);

**data processing by data processor:** any *data processing* performed by a *data processor* as commissioned or ordered by the *data controller*;

**data transfer:** disclosure of data for a specified *3rd party*;

**dissemination:** disclosure of data for non specified recipient (the general public);

**profiling:** any automated *processing of personal data*, which seeks the evaluation, analysis or prediction of personal aspects of the *data subject*;

**pseudonymisation:** the *processing of personal data* in such a manner that the *personal data* can no longer be attributed to a specific *data subject* without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the *personal data* are not attributed to an identified or identifiable natural person.

#### 4.1.4. Other terms

**consent of the data subject (abbr. consent):** any freely given, specific, informed and unambiguous indication of the *data subject's* wishes by which he or she, by a statement or

---

<sup>4</sup> The corresponding term in the Info law is “third person” (“harmadik személy”).

by a clear affirmative action, signifies agreement to the *processing of personal data* relating to him or her;

**filing system:** any structured set of *personal data* which are accessible according to specific criteria;

**data breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, *personal data* transmitted, stored or otherwise *processed*;

#### 4.1.5. Interpretation of international data processing

According to the 1st point of § 13 of the *Info law data transfer* to any EEA State or to Union institutions, bodies, offices and agencies as defined in chapters 4 and 5 of Title V of the Treaty on the Functioning of the European Union shall be considered the same as *data transfer* to recipients within Hungarian territory.

**cross-border processing of personal data within the EU:** *processing of personal data* within the European Union

- which takes place in the context of the activities of establishments in more than one Member State of a *data controller* or *data processor* in the Union where the *controller* or *processor* is established in more than one Member State; or
- which substantially affects or is likely to substantially affect *data subjects* in more than one Member State

**indirect data transfer:** disclosure of *personal data* to another *data controller* or *data processor* in a *third country* or under an *international organisation* by transmission of the *personal data* to a *data processor* or *data controller* in a *third country* or under an *international organisation*;

**international organisation:** an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

**EEA State:** a Member State of the European Union, or another contracting State to the Agreement on the European Economic Area, or any State that is not party to the Agreement on the European Economic Area who's Nationals are granted an equivalent legal status as the Nationals of a contracting State to the Agreement on the European Economic Area based on an international agreement with a Member State of the European Union;

**third country:** any State, which is not an EEA State

## 5. Details of the data processing

### 5.1. Logging related to the operation of the website

During the operation of the website the visit of the user is being logged for security purposes. Such logging may happen in two ways, which are different from *data processing* perspective too. We describe these shortly bellow and in more details later in this chapter.

- The logging of the visitors of the website
  - constitutes as *data processing*
  - the *data controller* is Slezsák Csilla SP
  - is necessary for the legitimate interest of the *controller*
  - affects every visitor

- the website offers no choice about it
- The logging related to services of the website provided by 3rd parties
  - constitutes as *data processing*
  - is necessary for the legitimate interest of the *controller*
  - the *data controller* is the 3rd party, e.g.: Google or Facebook
  - only affects visitors who give consent
  - the website prompts the visitor with a question
  - if rejected some features of the website may not work

### 5.1.1. The logging of the visitors of the Coconut Design Websites

Slezsák Csilla SP operates a public website under the domain names provided in chapter [2. Purpose and scope of this Privacy Policy](#) for those interested in their business and services.

For the operation of the website Slezsák Csilla SP – as the *data controller* with the previously declared contact details – performs *data processing* in the domain of access logging, of which details are provided below.

#### 5.1.1.1. The fact of the data processing

The Coconut Design Websites – similarly to the general common practice over the internet – maintain an access log for technical reasons. This means it automatically records the IP address of the visitor, the address of the page(s) being visited, the time and duration of the visit, and potentially the address of the website from where the visitor arrived to this website, the type of the client browser and other non-personal data.

The logging of these information happens continuously and automatically. During this *personal data* is being stored as listed below:

<b>Personal data</b>	<b>Purposes of the processing</b>	<b>Note of the Controller</b>
<b>IP address</b>	To be able to identify the visitor if needed.	The <i>data controller</i> and the <i>data processor</i> does never attempt to identify the visitors based on this information and they do not have the information required to do so. Such identification may only happen in cases where the applicable law or court orders to, and may only be performed by the appropriate public institutions based on additional information from internet service providers or other additional data sources.
<b>Referrer</b>	May contain <i>personal data</i> , if the visitor arrives from such an address (URL) which contains <i>personal data</i> (e.g.: email address).	The <i>data controller</i> and the <i>data processor</i> does never attempt to identify the visitors based on this information. Visitors of the website can ensure that no Referrer information is being stored if they open the website in a new window or an empty tab (i.e. not by clicking on a link). The Referrer field only contains the very previous address where the visitor is arrived from. Their browsing history is never transmitted during a visit to the site.

The *data controller* and the *data processor* does not connect this information with any other data sources and does never attempt to identify the visitors based on this information.

Slezsák Csilla SP does not *process* any other *personal data* in relation to the logging of the visitors during the operation of the website.

#### 5.1.1.2. The range of persons who are data subjects

Any user visiting the website.

The Access Log covers every website visits, so it affects every visitor of the website.

The Access Log does not differentiate between visitors by any means, so the *data processing* is not exclusive to natural persons visiting the website, but it happens for any other visits as well, e.g.: for page requests performed by automated means.

#### 5.1.1.3. Purposes of the processing

The purpose of this is to allow the identification and/or banning of those performing attacks or malicious page requests. Banning of visitors based on the data being *processed* can be done by both the *data controller* and the *data processor* without the identification of the visitor. Identification of the visitors shall only be performed by a competent authority in accordance with and under the safeguards provided by the applicable law.

#### 5.1.1.4. The legal basis of the data processing

##### 5.1.1.4.1. Determination of the basis of the data processing

Legitimate interest as defined under point (f) of paragraph 1 of Article 6 of GDPR:

“[Processing shall be lawful [...] if...] processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party [...]”

Obtaining a previous consent for the Access Log would involve disproportionate effort for both the *data controller* and the *data subjects* considering that the purpose of the logging is the tracking of the very access of the website. Since obtaining the consent online would require access prior to the consent is available, such consent may only be granted in another way (e.g.: by mail or phone). That is not lifelike and would practically render the website useless considering the fact that the purpose of the site is to provide quick and convenient way for access to information.

Since as described above the *data processing* under point (a) of paragraph 1 of Article 6 of GDPR cannot happen, and points (b) to (e) do not provide a suitable legal basis either, the *data processing* may only happen according to point (f) as necessary for the purposes of the legitimate interests.

To apply this legal basis the *data controller* should perform a Legitimate Interests Assessment. We provide the steps and the results of that below.

##### 5.1.1.4.2. Assessment of the legitimacy of the interest behind the data processing

It is a shared interest of both the *data controller* and the *data subjects* to ensure that the services offered on the website can be used in a secure and reliable manner and that attempts of fraud, abuse, disruption and blocking of the service can be prevented and avoided.

#### 5.1.1.4.3. Assessment of the necessity of the data processing

Data transmission and network connections between different computer systems and the large variety and variability of information technology equipments create such vulnerable points, which can be abused by IT hackers. World-wide best practice dictates the necessity of the usage this kind of logs in order to securely provide websites. Practically all website implements this solution to help with the secure operation. Based on that the *data controller* assumes it is a reasonable and necessary approach and if there was any better solutions to ensure the security of websites, there would be wide range of examples for the usage of such.

#### 5.1.1.4.4. Assessment of the impact for the data subjects and their interests

The data collected during this *data processing* are not sufficient to determine the identity of the *data subjects* unless information from other sources are used as well. The *data controller* and the *data processor* does NOT have access to such additional information. The identification of the *data subjects* – apart from the possibility of them willingly providing their identifiable information – shall only happen as part of proceedings by authorities as deemed required by the applicable law or as required in case of suspected criminal offences, but even in such cases the identification is not performed by the *data controller* or the *data processor*. Based on that if the service is used in good faith manner we can rule out any harm to the interests of the *data subject* in the context of the determination of their identity.

The referrer information collected during the *data processing* may contain *personal data* or information allowing of the determination of the identity of the *data subject*, however for the very reason this information is made available to the visited websites by most web browsers, any reasonably modern website would avoid putting *personal data* or personally identifiable information in such a way, that they may end up in the referrer field. If the *personal data* of the *data subject* appears in the referrer field, the browser would make that information available to any other visited websites as well, so in that case the risks for the *data subject* is not caused by the *data processing* described here, but rather caused by the insufficient technical execution of other services used by the *data subject* and by the lack of the implementation of other preventive measures on the *data subject's* behalf, such as the usage of private or incognito browsing or opening the website in a new window or on a new tab (which are easy ways to prevent the referrer information from being transmitted).

Beside the assessment of the effects for the *data subjects* and the probability of those effects (above) we also asses the severity of those effects in case they may happen. The most severe risk for the *data subjects* is that their identity may get discovered and someone who has access to the data can determine the fact that a particular *data subject* has visited the website. Since the *data controller* and the *data processors* commit to not give out this data to 3rd parties, and that the data is not used for any purpose other than the maintenance of the operation security of the website, and they also declare the lack of any additional information which would be required to determine the identity of the *data subjects*, there is no known, lifelike case in the context of this *data processing* which would cause disadvantage or harm to the interests of anyone, therefore the assessed risks are low in terms of their severity.

#### 5.1.1.4.5. The balance between the legitimate interest of the data controller and the protection of the interest of the data subjects

Based on the assessments performed above it can be determined, that the risk of harm to the interests of the *data subjects* and the severity of the consequences of a potentially harmful event are both low, and the widely adopted practices also suggest that the *data controller* is reasonable to assume the legitimate interest as the basis of the data handling as defined under point (f) of paragraph 1 of Article 6 of GDPR for the *data processing* associated with the Access Logs.



However if the *data subject* is not using the website service provided by the *data controller* in good faith, the interest in the prevention and investigation of the harmful or possibly criminal activities enjoys precedence over the interest of the suspected perpetrator to conceal their identity, so even in such case there is a justification for the *data processing*.

As the usage of access logs is a generally common practice for websites and other internet based public services, it is considered a reasonable expectation of the users to become the subject of such *data processing* in the context of the service described in this chapter. Based on that obtaining a previous consent for or providing prior information about the Access Log would not only involve disproportionate effort as described previously, but may also be unreasonable and unnecessary, more over annoying and unpleasant considering that nowadays the existence of access logs is common knowledge and we may expect the *data subjects* to be reasonably informed of that as a general fact about using the internet.

The *data controller* also points out that the period of time for which the data in the Access Logs is stored is no more than 2 (two) months. After that period of time the data – in case of no suspected criminal offences or cyber-attack – is deleted automatically, ensuring that the effects for the *data subjects* are not only constrained in terms of risks and the potential severity of breaches, but also in terms of the time frame.

The *data controller* draws attention to the fact that the *data subjects* may restrict the *data processing* described here by the appropriate configuration of their computers or devices used for web browsing or by utilising services helping with online anonymity, and doing so they may also better protect their interests and data in the context of other web based services independent from this website if they wish so.

#### 5.1.1.5. List of recipients and those entitled to access the data

The data obtained during the *data processing* is not accessible for the *data subjects*, only for the *data controller* and the *data processor*. The *data controller* respecting the stated principles prevents the access to the data without a sufficient cause.

The *data controller* or the *data processor* may hand over the log files to the appropriate authorities in case of suspected criminal offences, cyber-attacks or in case of any other cases if required by the applicable law.

Apart from that there are no recipients of the data stored in the log files, i.e. the *data controller* and the *data processor* does not disclose the stored data to anyone else.

#### 5.1.1.6. Time-frame of the data handling

Information stored in the Access Logs are kept in their original form for approximately 24 (twenty-four) hours. After that the contents of the files are archived. The archives are kept for a maximum of 2 (two) months<sup>5</sup>. After that the log entries are automatically deleted in an unrecoverable way.

---

<sup>5</sup> The archives of the logs from the previous month are automatically deleted at the last day of each month, so the shortest time log entries are stored is 1 month (for website visits on the last day of the month) and the longest time of storage is one day shorter than 2 months (60 days at maximum) (for website visits on the first day of the month).

Please note, that since the log archives are deleted on the last day of each month, the actual storage time of the log entries varies between 28 and 60 days depending on the length of the actual month and the day of the website access.

If, as soon as logs are transmitted to public authorities, any further *data processing* is going to be performed by those bodies acting within their own competence, and the *data controller* cannot be held responsible for the details of the further *processing* of the data. In such cases the time at which the data is deleted or the way the data is *processed* cannot be guaranteed within the context of this document.

#### 5.1.1.7. Clarification of the rights of the data subjects

The *data subjects* have all rights granted by the applicable law, of which we provide an overview in chapter [9. The rights of the data subjects](#) of this document.

On top of the generic information, the additional information provided below must be taken into account:

Modification to the stored data – considering the purpose of the logs is to record information exactly as it was at the time of the visits – is not possible without damaging the integrity and credibility of the data, therefore we cannot fulfil such requests.

Since the erasure of the data happens by an automated deletion setup, fulfilling requests to keep, transfer, disclose, lock or in any other way *process* the data may or may not be possible for records older than 1 (one) month, and is certainly impossible for records older than 2 (two) months.

Also according to paragraph 2 and 6 of Article 12 of GDPR requests for the retention, disclosure by transmission, transfer or other means of *data processing* can only be fulfilled if the *data subject* provides sufficient evidence that they had a given IP at the time of a given website visit. Alas without such evidence – since nor the *data controller* neither the *data processor* can determine the identity of the website visitors – we cannot provide access to or fulfil any requests regarding the data stored in the Access Logs.

#### 5.1.1.8. Data processors performing data processing

In the course of the provision of the website service the following hosting provider performs *data processing* as the *data processor*:

##### **GreenGeeks**

Principal address: 5739 Kanan Rd, Suite 300 Agoura Hills, CA 91301 USA

E-mail address: [support@greengeeks.com](mailto:support@greengeeks.com)

#### 5.1.1.9. Information about transfers of personal data to third countries or international organisations

GreenGeeks as a *data processor* serves the visitors and provides the service from their data centre located in the Netherlands, so the *personal data* of the *data subjects* are not transferred directly to *third countries* or *international organisations*.

However GreenGeeks, when it is essential for the provisioning of the service, may access the processed data from a third country. GreenGeeks provides the safeguards for the *data controller* and the *data subjects*, that they adhere to the regulations of GDPR as stated below:

- <https://www.greengeeks.com/legal/dpa> - especially under paragraphs 3/H and 3/I

## 5.1.2. The logging related to services of the website provided by 3rd parties

The *data processing* described below is optional and is based on a consent:

You can enable or disable these services and the related *data processing* using the buttons in the notification window shown on the website or using the buttons under the <https://coconutdesign.eu/privacy-policy/> address.

### 5.1.2.0.1. Important notice

Paragraph 1 of Article 7 of GDPR requires where *processing* is based on consent, the *controller* shall be able to demonstrate that the *data subject* has consented to *processing* of his or her *personal data*. Therefore the IP address and the client application signature (user agent) is being logged within the context of the consent for the users giving consent. The *data controller* does not use this data, alone or together with any other data, to determine the identity of the visitors. The purpose of the logging is sole to fulfil the above mentioned requirement of the GDPR. The IP address of users not giving consent is stored using a one way encoding (salted sha256), which prevents the access to the IP address. This way the IP address of the user cannot be determined, however in case of dispute it is possible to unambiguously determine if the user of a given IP address has declined the consent for the *data processing*. The user may avoid getting their data into this log by not clicking on neither the acceptance nor the decline of consent buttons. In that case the website functions just as if the user would have declined the consent to use services of the website provided by 3rd parties. Please note however, that some features of the website may be incomplete or unavailable without the consent.

### 5.1.2.1. The fact of the data processing

Since some parts of the website are based on using and/or embedding services provided by *3rd parties* (e.g.: analytic service) during the browsing of the website – in case the user has given consent – some parts are not served by the Coconut Design Websites, but other service providers. During that the browser of the user or device used for browsing does not only downloads content from the Coconut Design Websites, but also from the servers of those service providers. Similarly to the Coconut Design Websites those servers may has Access Logging enabled too, so the data of the user may appear in the logs on those servers as well.

For these services the Coconut Design Websites only act as a service-providing intermediary. The user always consumes these services from the respective providers, so in the context of these services the *data controller* is the provider of the service provisioned under the given domain name, and the relevant privacy policy regarding these logs are the ones of those service providers. Accordingly, the legal basis of the *data processing* can only be evaluated between the *data subject* and the given service providers as *data controller*, it is independent from the provider of this website and this *Privacy Policy*.

While the *data controller* for these services is not Slezsák Csilla SP, for the sake of greater transparency we provide the list of these services and service providers.

The parts of the Coconut Design Websites based on embedded 3rd party services are the following:

- Analytical data collection for statistical purposes (Google Analytics)
  - Service provider and data controller: Google Ireland Limited
  - Service: [Google Analytics](#)

- Code embedded in the website allowing for the customisation of advertisements (Facebook Pixel)
  - Service provider and data controller: Facebook Ireland Limited
  - Service: [Facebook Ads Pixel](#)

Precise information regarding the kind of *data processing* performed in the context of these services can be provided by the respective service providers. Below the location of the Privacy Policies of the service providers are listed, which may help you to obtain such information.

### Google Ireland Limited

Principal address: Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland

Location: [https://support.google.com/policies?p=privpol\\_privts](https://support.google.com/policies?p=privpol_privts)

Data processing information: <https://policies.google.com/privacy>

### Facebook Ireland Limited

Principal address: 4 Grand Canal Square, Grand Canal Harbour, Dublin, D02, Ireland

Location: <https://www.facebook.com/privacy/explanation> (bottom of the page)

Data processing information: <https://www.facebook.com/privacy/explanation>

#### 5.1.2.2. The range of persons who are data subjects

Data of the website visitors may get into these logs if both of the following criteria is true for them:

- **they have given consent to the usage of optional services when visiting the Coconut Design Websites,**
- **the given service provider has a legal basis for the *data processing*.**

While the consent is granted by the user, the consent may be given or denied for each software and device used by the same user independently. Since the provider of the website does not attempt to identify and match the separate software and devices used by the same user, the state of the consent may be different for different software and devices.

#### 5.1.2.3. Purposes of the processing

In all cases as determined by the given service provider as the *data controller*.

#### 5.1.2.4. The legal basis of the data processing

In all cases as determined by the given service provider as the *data controller*.

The legal basis of the given service provider may be the consent of the user (which is not the same as the consent given on the Coconut Design Websites, but it is an additional one given on the website or other contact points of the respective service provider), or another legal basis described in paragraph 1 of Article 6 of GDPR.

In practice it means, if you are a registered user of the services listed in this chapter, you are most likely given your consent to some *data processing* in the context of those services, so you are most likely a *data subject* – provided that you have also given consent to the usage of optional services when visiting the Coconut Design Websites.

If you have not given an explicit *data processing* consent for a service provider, but you have given consent to the usage of optional services when visiting the Coconut Design Websites, then according to the paragraph 1 of Article 6 of GDPR you may only become a *data subject* to the *data processing* described in this chapter in a legal way, when such *processing* is necessary for the

purposes of the legitimate interests pursued by the *data controller* or by a *3rd party*, except where such interests are overridden by the interests or fundamental rights and freedoms of the *data subject* which require protection of *personal data*.

#### 5.1.2.5. List of recipients and those entitled to access the data

In all cases as determined by the given service provider as the *data controller*.

#### 5.1.2.6. Time-frame of the data handling

In all cases as determined by the given service provider as the *data controller*.

#### 5.1.2.7. Clarification of the rights of the data subjects

The *data subjects* have all rights granted by the applicable law, of which we provide an overview in chapter [9. The rights of the data subjects](#) of this document.

Detailed information about the rights of the *data subjects* can be provided by the respective service provider as a *data controller*.

#### 5.1.2.8. Data processors performing data processing

In all cases as determined by the given service provider as the *data controller*.

#### 5.1.2.9. Information about transfers of personal data to third countries or international organisations

In all cases as determined by the given service provider as the *data controller*.

## 5.2. Handling of cookies related to the operation of the website

Slezsák Csilla SP operates a public website under the domain names provided in chapter [2. Purpose and scope of this Privacy Policy](#) for those interested in their business and services.

The technical execution of certain features on the website operated by Slezsák Csilla SP – as the *data controller* with the previously declared contact details – may require to store small data packets (so called cookies) on the computer of the user and to read the contents of those at the time of future visits. We provide information below about this technical solution as *data processing*.

### 5.2.1. Generic information about the cookies

If the user opens the Coconut Design Websites and meanwhile the browser software sends back a previously saved cookie, the provider handling the cookie can correlate the actual visit of the user with previous visits. Cookies may typically server the following purposes:

- improve the user experience;
- allow the personalisation of content shown for the user;
- remember the users personal settings and login details;
- may help the usage of the website (e.g.: there is no need to fill in recurring details in forms);
- collect information about the visitor and their devices, which can be used to improve and optimize the website;

- facilitate showing of advertisements relevant to the interests of the visitors during their browsing.

You can any time remove the cookies from your browser or device used for browsing. You can find more details about this in the help or users manual of the browser or device! Please note, that removing of cookies may cause problems when using certain websites.

**If you are making changes on your computer or other information technology device, always be careful and make a backup before performing the changes! Slezsák Csilla SP does not accept any responsibility for any consequences of changes made by you or a 3rd party on your computer or other information technology device!**

Some of the used cookies does not contain any *personal data*, and some does. Some of the cookies containing *personal data* are essential for the proper operation of the website, and some other, optional ones are aimed to provide some services optional for the site. Based on this classification there are fundamental differences between the handling of the cookies, so we discuss them separately:

- **Cookies not containing personal data:**
  - does not constitutes as *data processing* (since it contains no *personal data*)
  - affects all visitors (whose browser allows the usage of cookies)
  - the website offers no choice about it
- **Essential and session cookies containing personal data:**
  - constitutes as *data processing* (it contains *personal data*)
  - the *data controller* is Slezsák Csilla SP
  - is necessary for the legitimate interest of the *controller*
  - affects all visitors (whose browser allows the usage of cookies)
  - the website offers no choice about it
- **Cookies containing potentially personal data:**
  - partly constitutes as *data processing* (it may contain *personal data*)
  - the *data controller* is Slezsák Csilla SP
  - is based on the *data subject's* consent
  - only affects visitors who give *consent*
  - the website prompts the visitor with a question
  - if rejected some features of the website may not work
- **Optional cookies from 3rd parties:**
  - partly constitutes as *data processing* (it may contain *personal data*)
  - the *data controller* is the 3rd party (e.g.: Google or Facebook)
  - is based on the *data subject's* consent
  - only affects visitors who give *consent*
  - the website prompts the visitor with a question
  - if rejected some features of the website may not work

## 5.2.2. Cookies not containing personal data

### 5.2.2.1. The fact of the data processing (or the lack thereof)

These cookies do not constitute as *personal data*, since they contain no information, which could be used to determine the identity of the visitors in the sense of paragraph 1 of Article 4 of GDPR. Therefore **the usage of these cookies does not constitute as *data processing*** and visitors to the website who are subject to the usage of these cookies do not constitute as *data subjects*. Accordingly **there is no need to determine a legal basis for the usage of these cookies.**

The *data controller* declares, that they under no circumstances attempt to determine the identity of the visitors based on cookies, and they have no access to any additional information, with which correlating the data stored in the non-optional cookies would allow for the determination of the visitors identity.

While the usage of these cookies does not constitute as *data processing*, below we provide some of the information mandatory to be provided for *data processing* cases.

#### 5.2.2.2. The range of persons who are data subjects

Since there is no processing of *personal data* in the context of these cookies, there are no *data subjects* either as defined in the context of this document.

The cookies not containing *personal data* are stored and retrieved for those persons, whose browser and/or device used to visit the website is configured in a way, that allow for the website to handle cookies during and after the visit.

**Note:** The majority of the most common browser software and devices used for browsing nowadays by default allow the handling of cookies, so if you are visiting our website, you are most likely subject to the handling of these cookies.

#### 5.2.2.3. Purposes of the data processing

The purpose of these cookies is to allow the visitors to fully and smoothly browse the website, use its features and the services offered there. Some of these cookies are essential for the proper operation of the website, so the purpose of using these is to provide the functionalities of the website.

Bellow we present as well the purpose in more details for the individual cookies.

#### 5.2.2.4. List of recipients and those entitled to access the data

The data contained in the cookies in normal cases is only accessible for the *data controller*, the *data processor* (hosting provider) and those, who have access to the device storing the cookie.

There are no *recipients* of the data stored in the cookies, i.e. the *data controller* and the *data processor* does not disclose the stored data to anyone else.

The browser software usually by default and by design does not allow unauthorised websites or parties to read the cookies. However the cookies are always stored on the computer or information technology device of the visitors of the website. **Slezsák Csilla SP cannot and does not accept any responsibility for the security, integrity, correctness, availability or any other expectation related to the information stored on the device of the visitors of the website.**

#### 5.2.2.5. Duration of the data processing

The validity of the session type cookies lasts until the end of the session (browsing). These kind of cookies are automatically deleted from the computer or device used for browsing when the browser is closed. Some other cookies however are not deleted immediately after the end of the

browsing session. The time of erasure corresponding to these cookies are provided at the end of this chapter one by one.<sup>6</sup>

#### 5.2.2.6. Clarification of the rights of the data subjects

As described in chapter [5.2.2.2. The range of persons who are \*data subjects\*](#) there are no *data subjects* in the context of these cookies. The below need to be considered specifically for this case:

Since the cookies are stored on your device, you have every right to process this information, which you generally have to process any other information stored on your computer or information technology device, such as read, multiply, forward, modify, delete etc. the cookies or the information stored inside them.

Please note, that modifying or removing of cookies or their contents may cause problems when using certain websites!

**If you are making changes on your computer or other information technology device, always be careful and make a backup before performing the changes! Slezsák Csilla SP does not accept any responsibility for any consequences of changes made by you or a 3rd party on your computer or other information technology device!**

Please note, that the multiplication, insecure storage or sharing of cookies or the information stored in them entail security risks and may result in unauthorised access to your information or user accounts!

**Always be careful when copying or sharing data! Slezsák Csilla SP does not accept any responsibility for any consequences of activities of you or a 3rd party related to the cookies!**

Additionally we draw attention to the fact, that since the cookies and their contents are always stored on your device, the *data controller* has a limited capacity to *process* the data. The main limiting factor is that the *data controller* can only *process* the data in cases and at occasions when the browser or device of the user connects to the website, and even in that case only in ways allowed by the user's device. Considering this and paragraph 5 of Article 12 of GDPR any requests for measures described in Articles 15, 19 and 34 of GDPR are deemed unfounded, while requests for measures described in Articles 16-18 and 20 of GDPR can only be performed in limited ways and due to the complexity of the required technical solution can only be performed at a charge of high administrative costs, and only with the willing active cooperation of the requester.

#### 5.2.2.7. Data processors performing data processing

During the handling of cookies the following hosting provider performs handling of the cookies, but since the cookies does not contain *personal data*, in this context the following provider (or any other parties) does not qualify as *data processors*.

#### **GreenGeeks**

Principal address: 5739 Kanan Rd, Suite 300 Agoura Hills, CA 91301 USA

E-mail address: [support@greengeeks.com](mailto:support@greengeeks.com)

---

<sup>6</sup> The erasure of the cookies is not the responsibility of the *data controller*, but the device or software used for browsing, so in case of and uncommon configuration the storage time may be different from those stated in this document.



#### 5.2.2.8. List of cookies

- **Name of cookie:** ginger-cookie  
**Domain:** (www.)coconutdesign.eu  
**Description:** This cookie stores your decision about the usage of the optional cookies, If this cookie gets deleted, the website will ask for consent again!  
**Default storage time:** 1 year (after the last visit)
- **Name of cookie:** ginger-policy  
**Domain:** (www.)coconutdesign.eu  
**Description:** This cookies stores the version of the *Privacy Policy* in effect at the time of the consent is given. This is required, so users can change their consent of there are significant changes. If this cookie gets deleted, the website may ask for consent again!  
**Default storage time:** 1 year (after the last visit)

#### 5.2.3. Essential and session cookies containing personal data

##### 5.2.3.1. The fact of the data processing

In order to provide certain functions the Coconut Design Websites initiate the storage and retrieval of small data packets (so called cookies) on the computer of the user. These cookies, due to the information stored in them constitute as *personal data*, since they allow the determination of the identity of the *data subjects* in an indirect manner.

##### 5.2.3.2. The range of persons who are data subjects

The essential and session cookies containing *personal data* are stored and retrieved for those persons, whose browser or device used to visit the website is configured in a way, that allow for the website to handle cookies during and after the visit.

**Note:** The majority of the most common browser software and devices used for browsing nowadays by default allow the handling of cookies, so if you are visiting our website, you are most likely a *data subject* in the context of this *data processing*.

##### 5.2.3.3. Purposes of the processing

The purpose of these cookies is to allow the visitors to fully and smoothly browse the website, use its features and the services offered there.

The cookies used are essential for the proper operation of the website, since they play key roles in such information technology solutions, without which certain functions of the website could not, or only could be implemented, with data processing of a same extend implemented in a technically different way. Based on this the purpose of the *data processing* is to ensure the adequate functionality of the website.

Bellow we present as well the purpose in more details for the individual cookies.

##### 5.2.3.4. The legal basis of the data processing

###### 5.2.3.4.1. Determination of the basis of the data processing

Legitimate interest as defined under point (f) of paragraph 1 of Article 6 of GDPR:

“[Processing shall be lawful [...] if...] processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party [...]”

The coconutdesign.eu website uses information technology solutions, which improve the user experience and the ease of use of the functions offered on the website in such a way, that the part of the information, choices and preferences provided by or generated in the context of the users are stored in cookies to avoid their repeated input in the future. Since the storage of this information is necessary for the proper functioning of the website, obtaining explicit permission may only be possible, if the website would lock out visitors without consent. Such practice would render it impossible for the site to fulfil its original purpose, especially conveying information in a fast and convenient way.

Since as described above the *data processing* under point (a) of paragraph 1 of Article 6 of GDPR cannot happen, and points (b) to (e) do not provide a suitable legal basis either, the *data processing* may only happen according to point (f) as necessary for the purposes of the legitimate interests.

To apply this legal basis the *data controller* should perform a Legitimate Interests Assessment. We provide the steps and the results of that below.

#### 5.2.3.4.2. Assessment of the legitimacy of the interest behind the data processing

It is a shared interest of both the *data controller* and the *data subjects* to ensure that the website and the services offered on the website are of high quality, offer good usability and convenience, and also to avoid asking the visitors to repeatedly input certain information, preferences and decisions.

#### 5.2.3.4.3. Assessment of the necessity of the data processing

In order to store the information obtained for the *data subjects* the *data processing* is unavoidable. There are multiple technologies that may solve the storage of such information. Most of these solutions store the data on the systems of the *data controller*. On the contrary using of cookies is a solution, for which the data is not stored on the systems operated by the *data controller*. By storing the data on the data subject's system both the risks of abuse and the complexity of the *data processing* processes and methods can be reduced. Based on that, if we accept the necessity of storing these data, one of the best solution to reduce the risks of the *data subjects* is to store the information in cookies.

This is confirmed by the world-wide best practice as well, based on which it is clear that it is common to use some essential and session type cookies.

#### 5.2.3.4.4. Assessment of the impact for the data subjects and their interests

The data which is subject to this *data processing* is always stored on the device of the *data subject* used for the browsing. The *data controller* can only access this data, when the *data subject* is using the website of the *data controller*. While the storage time of the data may exceed the time of the usage of the website, if the *data subject* does not visit the website again within this time-frame – apart from the usage of a negligibly small storage space on their information technology device – no effects are arising for the *data subject*.

The effects for the *data subject* at the time of a repeated visit to the website may be:

- the website is able to “remember” the data and choices previously input by the *data subject*
- the website may be able to correlate the visit of the *data subject* visitor with previous visits, i.e. the website is able to recognise that the *data subject* has visited the website before
- the website becomes able to customise the services and content displayed and to uniquely personalise them based on the data generated during a previous visit or visits

The biggest risk for the *data subject* in this context, is that the *data controller* may become able to determine, that the *data subject* is the same person as another user who visited the website previously.

#### 5.2.3.4.5. The balance between the legitimate interest of the data controller and the protection of the interest of the data subjects

If the *data subject* only visits the website on a single occasion, at the end of the visit the *data processing* is either terminated (for session cookies) or it may continue in a technical sense (for cookies with a retention time longer than the session duration), however since the *data controller* cannot access the cookies without subsequent visits, there is no legitimate interest of the *data subject*, that would require the *data controller* to refrain from the *data processing* and the pursuit of their own legitimate interest as described above.

If the *data subject* visits the website multiple times, the balance of the interests can be assessed considering the following effects.

- benefits for the *data subject*:
  - the website is able to “recall” the previous preferences of the *data subject*, which makes using the website for the *data subject* easier, faster and more convenient,
  - the *data subject* may save time and effort,
- potentially unwanted effects for the *data subject*:
  - the *data controller* may become able to determine *data subject* is the same person as another user who visited the website previously
  - visiting the website may offer a different experience, content and conditions compared to what it would be like if they visited the site for the very first time
- benefits for the *data controller*:
  - the improved ease of use on the website improves the competitiveness of the provider of the website compared to other similar websites,
  - the improved ease of use on the website improves the satisfaction of the users of the website

Based on the assessments performed above it can be determined, that the risk of harm to the interests of the *data subjects* and the severity of the consequences of a potentially harmful event are both low, and the widely adopted practices also suggest that the *data controller* is reasonable to assume the legitimate interest as the basis of the data handling as defined under point (f) of paragraph 1 of Article 6 of GDPR for the data processing associated with the cookies referred to.

#### 5.2.3.5. List of recipients and those entitled to access the data

The data contained in the cookies in normal cases is only accessible for the *data controller*, the *data processor* (hosting provider) and those, who have access to the device storing the cookie.

There are no *recipients* of the data stored in the cookies, i.e. the *data controller* and the *data processor* does not disclose the stored data to anyone else.

The browser software usually by default and by design does not allow unauthorised websites or parties to read the cookies. However the cookies are always stored on the computer or information technology device of the visitors of the website. **Slezsák Csilla SP cannot and does not accept any responsibility for the security, integrity, correctness, availability or any other expectation related to the information stored on the device of the visitors of the website.**

#### 5.2.3.6. Time-frame of the data handling

The validity of the session type cookies lasts until the end of the session (browsing). These kind of cookies are automatically deleted from the computer or device used for browsing when the browser is closed. Some other cookies however are not deleted immediately after the end of the browsing. The time of erasure corresponding to these cookies are provided at the end of this chapter one by one.<sup>7</sup>

#### 5.2.3.7. Clarification of the rights of the data subjects

The *data subjects* have all rights granted by the applicable law, of which we provide an overview in chapter [9. The rights of the data subjects](#) of this document.

On top of the generic information, the additional information provided below must be taken into account:

Since the cookies are stored on the device of the *data subject*, the *data subject* has every right to process this information, which one generally have to process any other information stored on their computer or information technology device, such as read, multiply, forward, modify, delete etc. the cookies or the information stored inside them.

Please note, that modifying or removing of cookies or their contents may cause problems when using certain websites!

**If you are making changes on your computer or other information technology device, always be careful and make a backup before performing the changes! Slezsák Csilla SP does not accept any responsibility for any consequences of changes made by you or a 3rd party on your computer or other information technology device!**

Please note, that the multiplication, insecure storage or sharing of cookies or the information stored in them entail security risks and may result in unauthorised access to your information or user accounts!

**Always be careful when copying or sharing data! Slezsák Csilla SP does not accept any responsibility for any consequences of activities of you or a 3rd party related to the cookies!**

Additionally we draw attention to the fact, that since the cookies and their contents are always stored on the device of the *data subject*, the *data controller* has a limited capacity to *process* the data. The main limiting factor is that the *data controller* can only process the data in cases and at occasions when the browser or device of the user connects to the website, and even in that case only in ways allowed by the user's device. Considering this and paragraph 5 of Article 12 of GDPR any requests for measures described in Articles 15, 19 and 34 of GDPR are deemed unfounded, while requests for measures described in Articles 16-18 and 20 of GDPR can only be performed in limited ways and due to the complexity of the required technical solution can only be performed at a charge of high administrative costs, and only with the willing active cooperation of the *data subject*.

---

<sup>7</sup> The erasure of the cookies is not the responsibility of the *data controller*, but the device or software used for browsing, so in case of and uncommon configuration the storage time may be different from those stated in this document.

#### 5.2.3.8. Data processors performing data processing

During the handling of cookies the following hosting provider as a *data processor* performs *data processing* for the cookies

##### **GreenGeeks**

Principal address: 5739 Kanan Rd, Suite 300 Agoura Hills, CA 91301 USA

E-mail address: [support@greengeeks.com](mailto:support@greengeeks.com)

#### 5.2.3.9. Information about transfers of personal data to third countries or international organisations

GreenGeeks as a *data processor* serves the visitors and provides the service from their data centre located in the Netherlands, so the *personal data* of the *data subjects* are not transferred directly to *third countries* or *international organisations*.

However GreenGeeks, when it is essential for the provisioning of the service, may access the processed data from a *third country*. GreenGeeks provides the safeguards for the *data controller* and the *data subjects*, that they adhere to the regulations of GDPR as stated below:

- <https://www.greengeeks.com/legal/dpa> - especially under paragraphs 3/H and 3/I

#### 5.2.3.10. List of cookies

- **Name of cookie:** woocommerce\_items\_in\_cart  
**Domain:** coconutdesign.eu  
**Description:** Stores the items in the shopping cart.  
**Default storage time:** session duration
- **Name of cookie:** woocommerce\_cart\_hash  
**Domain:** coconutdesign.eu  
**Description:** Identifies the data associated with the shopping cart.  
**Default storage time:** session duration

#### 5.2.4. Cookies containing potentially personal data

The *data processing* described below is optional and is based on a consent:

You can enable or disable these services and the related *data processing* using the buttons in the notification window shown on the website or using the buttons under the <https://coconutdesign.eu/privacy-policy/> address.

The attention of *data subjects* is drawn to the fact, that the *data processing* for the behaviour based advertisement service of Facebook can be controlled independently from the cookies used on this website as well, for example using

- the [Ad Choices](#) service or
- the [YourAdChoices](#) service.

The benefit of this is that you can refuse to consent to the *data processing* for the purpose of behaviour based advertisements even if you would like to give consent to the rest of the *data processing* on this website.

#### 5.2.4.0.1. Important notice:

Paragraph 1 of Article 7 of GDPR requires where *processing* is based on consent, the *controller* shall be able to demonstrate that the *data subject* has consented to *processing* of his or her personal data. Therefore the IP address and the client application signature (user agent) is being logged within the context of the consent for the users giving consent. The *data controller* does not use this data, alone or together with any other data, to determine the identity of the visitors. The purpose of the logging is sole to fulfil the above mentioned requirement of the GDPR. The IP address of users not giving consent is stored using a one way encoding (salted sha256), which prevents the access to the IP address. This way the IP address of the user cannot be determined, however in case of dispute it is possible to unambiguously determine if the user of a given IP address has declined the consent for the data handling. The user may avoid getting their data into this log by not clicking on neither the acceptance or the decline of consent buttons. In that case the website functions just as if the user would have declined the consent. Please note however, that some features of the website may be incomplete or unavailable without accepting these cookies.

#### 5.2.4.1. The fact of the data processing

In order to provide certain functions the Coconut Design Websites and some embedded parts and services of the website obtained from other service providers initiate the storage and retrieval of small data packets (so called cookies) on the computer of the user. These cookies, due to the information stored in them may constitute as *personal data*, since they in some cases allow the determination of the identity of the *data subjects* in an indirect manner.

#### 5.2.4.2. The range of persons who are data subjects

The cookies containing potentially *personal data* are stored and retrieved for those persons, who give consent to the usage of these cookies when visiting the website and whose browser or device used to visit the website is configured in a way, that allow for the website to handle cookies during and after the visit.

While the consent is granted by the user, the consent may be given or denied for each software and device used by the same user independently. Since the provider of the website does not attempt to identify and match the separate software and devices used by the same user, the state of the consent may be different for different software and devices.

#### 5.2.4.3. Purposes of the processing

Purpose of these cookies:

- on one hand to allow the visitors to fully and smoothly browse the website, use its features and the services offered there,
- on the other hand to enable the display of (behaviour based) personalised advertisements to the visitors which are relevant to their interests during their future browsing (Facebook retargeting).

These cookies are not essential for the proper operation of the website, since the basic functionality of the website is available for the visitors even without these, but it is recommended to accept them to achieve the full user experience.

Bellow we present as well the purpose in more details for the individual cookies.

#### 5.2.4.4. The legal basis of the data processing

The legal basis of the *data processing* is the consent of the *data subject* as defined under point (a) of paragraph 1 of Article 6 of GDPR:

“[Processing shall be lawful [...] if...] the data subject has given consent to the processing of his or her personal data [...]”

#### 5.2.4.5. List of recipients and those entitled to access the data

The data contained in the cookies in normal cases is only accessible for the *data controller*, the *data processor* (hosting provider and the providers of the embedded services) and those, who have access to the device storing the cookie.

There are no recipients of the data stored in the cookies, i.e. the *data controller* and the *data processor* does not disclose the stored data to anyone else.

The browser software usually by default and by design does not allow unauthorised websites or parties to read the cookies. However the cookies are always stored on the computer or information technology device of the visitors of the website. **Slezsák Csilla SP cannot and does not accept any responsibility for the security, integrity, correctness, availability or any other expectation related to the information stored on the device of the visitors of the website.**

#### 5.2.4.6. Time-frame of the data handling

The validity of the session type cookies lasts until the end of the session (browsing). These kind of cookies are automatically deleted from the computer or device used for browsing when the browser is closed. Some other cookies however are not deleted immediately after the end of the browsing. The time of erasure corresponding to these cookies are provided below one by one.<sup>8</sup>

#### 5.2.4.7. Clarification of the rights of the data subjects

The *data subjects* have all rights granted by the applicable law, of which we provide an overview in chapter [9. The rights of the data subjects](#) of this document.

On top of the generic information, the additional information provided below must be taken into account:

Since the cookies are stored on the device of the *data subject*, the *data subject* has every right to process this information, which one generally have to process any other information stored on their computer or information technology device, such as read, multiply, forward, modify, delete etc. the cookies or the information stored inside them.

Please note, that modifying or removing of cookies or their contents may cause problems when using certain.

**If you are making changes on your computer or other information technology device, always be careful and make a backup before performing the changes! Slezsák Csilla SP does not accept any responsibility for any consequences of changes made by you or a 3rd party on your computer or other information technology device!**

---

<sup>8</sup> The erasure of the cookies is not the responsibility of the data controller, but the device or software used for browsing, so in case of and uncommon configuration the storage time may be different from those stated in this document.

Please note, that the multiplication, insecure storage or sharing of cookies or the information stored in them entail security risks and may result in unauthorised access to your information or user accounts!

**Always be careful when copying or sharing data! Slezsák Csilla SP does not accept any responsibility for any consequences of activities of you or a 3rd party related to the cookies!**

Additionally we draw attention to the fact, that since the cookies and their contents are always stored on the device of the *data subject*, the *data controller* has a limited capacity to process the data. The main limiting factor is that the *data controller* can only *process* the data in cases and at occasions when the browser or device of the user connects to the website, and even in that case only in ways allowed by the user's device. Considering this and paragraph 5 of Article 12 of GDPR any requests for measures described in Articles 15 and 34 of GDPR are deemed unfounded, while requests for measures described in Articles 16-18 and 20 of GDPR can only be performed in limited ways and due to the complexity of the required technical solution can only be performed at a charge of high administrative costs, and only with the willing active cooperation of the *data subject*.

Moreover some cookies are not set by the *data controller*, but by the *data processors* using their own domain names, therefore the *data controller* is technically unable to apply any measures for those. Considering this and paragraph 5 of Article 12 of GDPR any requests regarding such cookies for measures described in Articles 15-18, 20 and 34 of GDPR are deemed unfounded by the *data controller*. The domain name for the cookies can be found in the detailed list of the cookies below.

#### 5.2.4.8. Data processors performing data processing

In the the course of the provision of the website service the following hosting provider performs *data processing* as a *data processor*:

##### **GreenGeeks**

Principal address: 5739 Kanan Rd, Suite 300 Agoura Hills, CA 91301 USA

E-mail address: [support@greengeeks.com](mailto:support@greengeeks.com)

On top of this, the *data controllers* listed below also perform *data processing* in relation to the cookies containing potentially *personal data* described in this chapter:

##### **Google Ireland Limited**

Principal address: Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland

Location: [https://support.google.com/policies?p=privpol\\_privts](https://support.google.com/policies?p=privpol_privts)

Data processing terms: [https://gsuite.google.com/terms/dpa\\_terms.html](https://gsuite.google.com/terms/dpa_terms.html)

##### **Facebook Ireland Limited**

Principal address: 4 Grand Canal Square, Grand Canal Harbour, Dublin, D02, Ireland

Location: <https://www.facebook.com/privacy/explanation> (bottom of the page)

Data processing terms: <https://www.facebook.com/legal/terms/dataprocessing>



#### 5.2.4.9. Information about transfers of personal data to third countries or international organisations

GreenGeeks as a *data processor* serves the visitors and provides the service from their data centre located in the Netherlands, so the *personal data* of the *data subjects* are not transferred to *third countries* or *international organisations*.

However GreenGeeks, when it is essential for the provisioning of the service, may access the processed data from a *third country*. GreenGeeks provides the safeguards for the *data controller* and the *data subjects*, that they adhere to the regulations of GDPR as stated below:

- <https://www.greengeeks.com/legal/dpa> - especially under paragraphs 3/H and 3/I

Google and Facebook provide their services within the European Union through their subsidiaries located in Ireland, so the *personal data* of the *data subjects* are not transferred directly to *third countries* or *international organisations*. At the same time the attention of *data subjects* is drawn to the fact that these organisations provide the safeguards for the *data controller* and the *data subjects* to not transfer the *personal data* of the *data subjects* to *third countries* or *international organisations* as stated below:

- Facebook: <https://www.facebook.com/about/privacysshield>
- Google: <https://policies.google.com/privacy/frameworks>

#### 5.2.4.10. List of cookies

The *data controller* performs *data processing* through *data processors* as described in this chapter for the cookies listed below:

- **Name of cookie:** NID  
**Domain:** google.com  
**Data processor:** Google  
**Description:** The browser of most Google user stores the settings related cookie named „NID”. The browser sends this cookie with requests addressed to the websites of Google. The NID cookie contains a unique identifier, which is used by Google to store your preferences – such as preferred language (e.g.: Hungarian), preferred number of search results (e.g. 10 or 20) or if you'd like to use Google's safe search filter – and other data.  
**Default storage time:** 6 months  
**Further information:** <https://policies.google.com/technologies/types>
- **Name of cookie:** fr  
**Domain:** facebook.com  
**Data processor:** Facebook  
**Description:** Used to identify the browser of the user, primarily used by Facebook to serve personalised advertisements.  
**Default storage time:** 3 months

#### 5.2.5. Optional cookies from 3rd parties

The data processing described below is optional and is based on a consent:

You can enable or disable these services and the related *data processing* using the buttons in the notification window shown on the website or using the buttons under the <https://coconutdesign.eu/privacy-policy/> address

#### 5.2.5.0.1. Important notice:

Paragraph 1 of Article 7 of GDPR requires where *processing* is based on consent, the *controller* shall be able to demonstrate that the *data subject* has consented to *processing* of his or her *personal data*. Therefore the IP address and the client application signature (user agent) is being logged within the context of the consent for the users giving consent. The *data controller* does not use this data, alone or together with any other data, to determine the identity of the visitors. The purpose of the logging is sole to fulfil the above mentioned requirement of the GDPR. The IP address of users not giving consent is stored using a one way encoding (salted sha256), which prevents the access to the IP address. This way the IP address of the user cannot be determined, however in case of dispute it is possible to unambiguously determine if the user of a given IP address has declined the consent for the data handling. The user may avoid getting their data into this log by not clicking on neither the acceptance or the decline of consent buttons. In that case the website functions just as if the user would have declined the consent. Please note however, that some features of the website may be incomplete or unavailable without these cookies!

#### 5.2.5.1. The fact of the data processing

Some embedded parts and services of the Coconut Design Websites obtained from other service providers initiate the storage and retrieval of small data packets (so called cookies) on the computer of the user. These cookies, due to the information stored in them may constitute as personal data, since they in some cases allow the determination of the identity of the data subjects in an indirect manner.

**The *data controller* draws the attention of the visitors** to the fact that the according to the standard defining the technical implementation of cookies (RFC 6265) some, previously mentioned *data controllers* may inevitably become able to process cookies as well, that – **opposed to the cookies described in the previous chapter** – are not set through or in the context of the Coconut Design Websites, but are available under the domain name of the given service provider.

Related to these cookies however the provider of the service under the given domain name does not act as a *data processor* but as a *data controller*. Thus regarding these cookies the *data controller* is not Slezsák Csilla SP, therefore these are not subject of this *Privacy Policy*. For the sake of greater transparency however we provide the most common information and the list of the most common such cookies below.

It is important to note, that regarding these cookies the *data controller* is the provider of the service provisioned under the given domain name, and the relevant privacy policy regarding these cookies are the ones of those service providers. Accordingly, the legal basis of the *data processing* can only be evaluated between the *data subject* and the given service providers as *data controllers*; it is independent from the provider of this website and this *Privacy Policy*.

A simple example of such situation may be, that while the Coconut Design Websites do not provide a way to log in to the Google Maps service using a Google Account, users, who previously consented to the use of cookies for google.com and has logged into the service would find that they are logged in with their Google user account within the map embedded on this website. The benefit of that is that the logged in user can access the additional services available within the given system, for example they can easily save a location into their bookmarks. However at the same time it also means, that Google becomes able to identify the visitor of the Coconut Design Websites and can recognise that a given Google user has visited the Coconut Design Websites.

In general terms so based on the cookies below users of the Coconut Design Websites may become identifiable in the context of the provider of the given service as *data controller* independently from the *data processing* performed on the Coconut Design Websites. Such identification may be used by the given service provider independently from the terms of this *Privacy Policy* for example to track the habits of the given user, to serve them targeted advertisements or other purposes.

Precise information regarding the kind of *data processing* performed in the context of these cookies can be provided by the respective service providers. Below the location of the Privacy Policies of the service providers are listed, which may help you to obtain such information.

### **Google Ireland Limited**

Principal address: Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland

Location: [https://support.google.com/policies?p=privpol\\_privts](https://support.google.com/policies?p=privpol_privts)

Data processing information: <https://policies.google.com/privacy>

### **Facebook Ireland Limited**

Principal address: 4 Grand Canal Square, Grand Canal Harbour, Dublin, D02, Ireland

Location: <https://www.facebook.com/privacy/explanation> (bottom of the page)

Data processing information: <https://www.facebook.com/privacy/explanation>

#### 5.2.5.2. The range of persons who are data subjects

These optional cookies may be lawfully set and retrieved for users of the website if **all three** of the following criteria is true for them:

- **they have given consent to the usage of optional cookies when visiting the Coconut Design Websites,**
- **the given service provider has a legal basis for the *data processing*, and**
- whose browser or device used to visit the website is configured in a way, that allow for the website to handle cookies during and after the visit.

#### 5.2.5.3. Purposes of the processing

In all cases as determined by the given service provider as the *data controller*, as well as described for the cookies in the list at the end of this chapter.

#### 5.2.5.4. The legal basis of the data processing

In all cases as determined by the given service provider as the *data controller*.

The legal basis of the given service provider may be the consent of the user (which is not the same as the consent given on the Coconut Design Websites, but it is an additional one given on the website or other contact points of the respective service provider), or another legal basis described in paragraph 1 of Article 6 of GDPR.

In practice it means, if you are a registered user of the services listed in this chapter, you are most likely given your consent to some *data processing* in the context of those services, so you are most likely a *data subject* – provided that you have also given consent to the usage of optional cookies when visiting the Coconut Design Websites.

If you have not given an explicit data processing consent for a service provider, but you have given consent to the usage of optional cookies when visiting the Coconut Design Websites, then according to the paragraph 1 of Article 6 of GDPR you may only become a *data subject* to the *data*

*processing* described in this chapter in a legal way, when processing is necessary for the purposes of the legitimate interests pursued by the service provider as the *data controller* or by a *third party*, except where such interests are overridden by the interests or fundamental rights and freedoms of the *data subject* which require protection of *personal data*.

#### 5.2.5.5. List of recipients and those entitled to access the data

In all cases as determined by the given service provider as the *data controller*.

#### 5.2.5.6. Time-frame of the data handling

In all cases as determined by the given service provider as the *data controller*, as well as described for the cookies in the list at the end of this chapter.

#### 5.2.5.7. Clarification of the rights of the data subjects

The data subjects have all rights granted by the applicable law, of which we provide an overview in chapter [9. The rights of the data subjects](#) of this document.

Detailed information about the rights of the *data subjects* can be provided by the respective service provider as a *data controller*.

#### 5.2.5.8. Data processors performing data processing

In all cases as determined by the given service provider as the *data controller*.

#### 5.2.5.9. Information about transfers of personal data to third countries or international organisations

In all cases as determined by the given service provider as the *data controller*.

#### 5.2.5.10. List of cookies

The service providers as data controllers typically perform *data processing* as described in this chapter for the cookies listed below:

- **Name of cookies:** SID, HSID, SSID, APISID, SAPISID, SIDCC  
**Domain:** google.com  
**Data controller:** Google  
**Description:** For logged in users of Google these serve for the identification and storage of login status. The purpose of these cookies is to store the digitally signed and encrypted data related to the Google Account and the timestamp of the last login. Google is able to prevent several cyber-attacks using these cookies, for example attempts to steal details filled in on web based forms.  
**Default storage time:** SIDCC: approx. 3 months, others: 23 months  
**Further information:** <https://policies.google.com/technologies/types>
- **Name of cookies:** \_gat, \_gid, \_ga  
**Domain:** google.com  
**Data controller:** Google  
**Description:** These cookies are required for functions of data collection for statistical purposes by Google Analytics.  
**Default storage time:** \_gat: 1 minute, \_gid: 24 hours, \_ga: 2 years  
**Further information:** <https://developers.google.com/>

- **Name of cookie:** CONSENT  
**Domain:** google.com  
**Data controller:** Google  
**Description:** A cookies used by Google, which does not directly contribute to the workings of this website, but Google uses it in some cases during the provisioning of their services.  
**Default storage time:** approx. 19 years.
- **Name of cookie:** 1P\_JAR  
**Domain:** google.com  
**Data controller:** Google  
**Description:** A cookies used by Google, which does not directly contribute to the workings of this website, but Google uses it in some cases during the provisioning of their services.  
**Default storage time:** 1 month
- **Name of cookie:** datr  
**Domain:** facebook.com  
**Data controller:** Facebook  
**Description:** Provides security services in the context of Facebook, which among other things helps to prevent the registration of fake profiles, helps to prevent the unauthorised acquisition and usage of Facebook accounts and in the protection against the s.c. DDoS attacks as well.  
**Default storage time:** 2 years
- **Name of cookie:** sb  
**Domain:** facebook.com  
**Data controller:** Facebook  
**Description:** Used by Facebook to improve recommendations in the friend suggestion systems.  
**Default storage time:** 2 years
- **Name of cookie:** c\_user  
**Domain:** facebook.com  
**Data controller:** Facebook  
**Description:** Serves to identify Facebook users.  
**Default storage time:** 3 months
- **Name of cookie:** xs  
**Domain:** facebook.com  
**Data controller:** Facebook  
**Description:** A session cookie which primarily serves to track the login status of users in the context of the embedded Facebook features and the sharing service.  
**Default storage time:** 3 months
- **Name of cookie:** pl  
**Domain:** facebook.com  
**Data controller:** Facebook  
**Description:** A cookies used in the context of the embedded Facebook features and the sharing service.  
**Default storage time:** 3 months

Please note that the list above is only intended for informational purposes and the given service providers may change the list of cookies being used. The exact list can at all times obtained from the given service provider as the *data controller*.

## 5.3. Other data processing related to the operation of the website

### 5.3.1. Other data processing related to services of the website provided by 3rd parties

The *data processing* described below is optional and is based on a consent:

You can enable or disable these services and the related *data processing* using the buttons in the notification window shown on the website or using the buttons under the <https://coconutdesign.eu/privacy-policy/> address.

#### 5.3.1.0.1. Important notice:

Paragraph 1 of Article 7 of GDPR requires where *processing* is based on consent, the *controller* shall be able to demonstrate that the *data subject* has consented to *processing* of his or her *personal data*. Therefore the IP address and the client application signature (user agent) is being logged within the context of the consent for the users giving consent. The *data controller* does not use this data, alone or together with any other data, to determine the identity of the visitors. The purpose of the logging is sole to fulfil the above mentioned requirement of the GDPR. The IP address of users not giving consent is stored using a one way encoding (salted sha256), which prevents the access to the IP address. This way the IP address of the user cannot be determined, however in case of dispute it is possible to unambiguously determine if the user of a given IP address has declined the consent for the data handling. The user may avoid getting their data into this log by not clicking on neither the acceptance or the decline of consent buttons. In that case the website functions just as if the user would have declined the consent. Please note however, that some features of the website may be incomplete or unavailable without these cookies!

#### 5.3.1.1. The fact of the data processing

Since parts of the website are built by embedding services provided by 3rd parties (e.g.: map) during the browsing of the website – in case the user has given consent – some parts are not served by the Coconut Design Websites, but other service providers.

For these services the Coconut Design Websites only acts as a service-providing intermediary. The user always consumes these services from the respective providers, so in the context of these services the *data controller* is the provider of the given service, and the relevant privacy policy regarding these logs are the ones of those service providers. Accordingly, the legal basis of the *data processing* can only be evaluated between the *data subject* and the given service providers as *data controllers*; it is independent from the provider of this website and this *Privacy Policy*.

While the *data controller* for these services is not Slezsák Csilla SP, for the sake of greater transparency we provide the list of these services and service providers.

The parts of the Coconut Design Websites based on embedded 3rd party services are the following:

- Analytical data collection for statistical purposes (Google Analytics)
  - Service provider and *data controller*: Google
  - Service: [Google Analytics](#)

Precise information regarding the kind of *data processing* performed in the context of these services can be provided by the respective service providers. Below the location of the Privacy Policies of the service providers are listed, which may help you to obtain such information.

### **Google Ireland Limited**

Principal address: Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland

Location: [https://support.google.com/policies?p=privpol\\_privts](https://support.google.com/policies?p=privpol_privts)

Data processing information: <https://policies.google.com/privacy>

#### 5.3.1.2. The range of persons who are data subjects

Website visitors may become data subjects if **both** of the following criteria is true for them:

- **they have given consent to the usage of optional services when visiting the Coconut Design Websites,**
- **the given service provider has a legal basis for the *data processing*.**

#### 5.3.1.3. Purposes of the processing

In all cases as determined by the given service provider as the *data controller*.

#### 5.3.1.4. The legal basis of the data processing

In all cases as determined by the given service provider as the *data controller*.

The legal basis of the given service provider may be the consent of the user (which is not the same as the consent given on the Coconut Design Websites, but it is an additional one given on the website or other contact points of the respective service provider), or another legal basis described in paragraph 1 of Article 6 of GDPR.

In practice it means, if you are a registered user of the services listed in this chapter, you are most likely given your consent to some *data processing* in the context of those services, so you are most likely a *data subject* – provided that you have also given consent to the usage of optional services when visiting the Coconut Design Websites.

If you have not given an explicit *data processing* consent for a service provider, but you have given consent to the usage of optional services when visiting the Coconut Design Websites, then according to the paragraph 1 of Article 6 of GDPR you may only become a *data subject* to the *data processing* described in this chapter in a legal way, when *processing* is necessary for the purposes of the legitimate interests pursued by the service provider as the *data controller* or by a *third party*, except where such interests are overridden by the interests or fundamental rights and freedoms of the *data subject* which require protection of *personal data*.

#### 5.3.1.5. List of recipients and those entitled to access the data

In all cases as determined by the given service provider as the *data controller*.

#### 5.3.1.6. Time-frame of the data handling

In all cases as determined by the given service provider as the *data controller*.

#### 5.3.1.7. Clarification of the rights of the data subjects

The data subjects have all rights granted by the applicable law, of which we provide an overview in chapter [9. The rights of the data subjects](#) of this document.

Detailed information about the rights of the *data subjects* can be provided by the respective service provider as a *data controller*.

#### 5.3.1.8. Data processors performing data processing

In all cases as determined by the given service provider as the *data controller*.

#### 5.3.1.9. Information about transfers of personal data to third countries or international organisations

In all cases as determined by the given service provider as the *data controller*.

### 5.3.2. Data processing related to the webshop service

The *data processing* described below is optional and is based on a consent: The consent is always given by the user (customer) in case of the orders submitted in the webshop by checking the relevant checkbox and in case of the delivery by selecting the service provider.

#### 5.3.2.0.1. Important notice:

Paragraph 1 of Article 7 of GDPR requires where *processing* is based on consent, the *controller* shall be able to demonstrate that the *data subject* has consented to processing of his or her personal data. For this reason the data required to identify the consenting user is stored based on the personal details provided during the purchase.

#### 5.3.2.1. The fact of the data processing

Slezsák Csilla SP (provider) operates a webshop (a shop without a physical place allowing to initiate purchases) within the Coconut Design Websites. To enable the fulfilment of the orders submitted in the webshop it is necessary to store some data related to the customers. Part of these information constitutes *personal data* based on its nature, since

- some of them are directly concerned with the identity of the *data subject* users (e.g. name and address),
- some of them may be sufficient to indirectly determine the identity of the *data subjects* (e.g. email address, phone number).

#### 5.3.2.2. The range of persons who are data subjects

In the context of the operation of the webshop the *processing of personal data* happens for the persons, who

- initiate an order in the webshop, and
- voluntarily provide their data, and
- give their consent for the *processing* of the provided data.

Whereas the *data controller* may be authorized to the *processing* of the *personal data* of the *data subject* users during subsequent orders based on the consent given at the time of their first order, in order to technically simplify the webshop (to avoid the mandatory user registration for purchases) the operator of the shop may ask for the consent for each order separately.

#### 5.3.2.3. Purposes of the processing

The purpose of the processing is to be able to properly and contractually fulfil the orders submitted in the webshop and for the operator to be able to fulfil its lawful duties (e.g. invoicing).



The *data processing* furthermore enables the provider of the webshop to implement discounts, promotions and to offer price reductions for customers based on their previous orders and the data related to those.

#### 5.3.2.4. The legal basis of the data processing

The legal basis of the *data processing* is the consent of the *data subject* as defined under point (a) of paragraph 1 of Article 6 of GDPR:

“[Processing shall be lawful [...] if...] the data subject has given consent to the processing of his or her personal data [...]”

#### 5.3.2.5. List of recipients and those entitled to access the data

The data related to the orders are primarily accessible by the *data controller* and the *data processors* (hosting provider).

##### 5.3.2.5.1. Additional data processors potentially processing data during the fulfilment of orders

For the fulfilment of the orders it may become necessary to transfer some *personal data* of the customer to a 3rd party as described below:

- During the fulfilment of the order, the *data controller* discloses the information of the customer to the extent necessary for the delivery for the postal or courier service provider or other 3rd parties participating in the shipping of the order.
- During the checkout process, for online payment the *data controller* uses the services of a 3rd party, and for this the details of the *data subject* necessary for the completion of the transaction are disclosed to the party handling the payment.

**The service provider** of the webshop however cannot guarantee the *data processing* practices of the 3rd parties providing delivery and payment services, so **particularly draws the attention of the customers to only accept the terms described in this *Privacy Policy*** and only submit orders in the webshop, **if they agree and consent to the forwarding of their data** in the context of their chosen shipment and payment methods.

For the postal and courier services and the online payment solutions the provider of the Coconut Design Websites only act as a service-providing intermediary. The user always consumes these services from the respective providers, so in the context of these services the *data controller* is the provider of the given service, and the relevant privacy policy regarding these services are the ones of those service providers. Accordingly, the legal basis of the *data processing* can only be evaluated between the *data subject* and the given service providers as *data controllers*; it is independent from the provider of this website and this *Privacy Policy*.

Precise information regarding the kind of *data processing* performed in the context of these services can be provided by the respective service providers. Below the location of the Privacy Policies of the service providers are listed, which may help you to obtain such information.

#### **Magyar Posta Zrt.**

Principal address: HUNGARY, 1138 Budapest, Dunavirág utca 2-6., Magyarország

Location: <https://www.posta.hu/>

Data processing information: [https://www.posta.hu/adatkezelesi\\_tajekoztato#2](https://www.posta.hu/adatkezelesi_tajekoztato#2).

#### **PayPal (Europe) S.à.r.l. et Cie, S.C.A.**

Principal address: 22-24 Boulevard Royal L-2449, Luxembourg

Location: <https://www.paypal.com/hu/smarthelp/contact-us>

Data processing information: <https://www.paypal.com/hu/webapps/mpp/ua/privacy-full>

#### 5.3.2.6. Time-frame of the data handling

The *data processor* stores the data related to the orders as long as any of the following criteria is true:

- the fulfilment (or the cancellation) of the order haven't been completed yet
- there may be additional administrative tasks to be completed after the fulfilment of the order, which require the storage of the data, such as:
  - the withdrawal is still possible for the given purchase or the processing of a withdrawal is in progress
  - the sold product is still under warranty or similar terms
  - there are administrative or management operations, coordination, dispute, lawsuit or other proceedings in progress for the benefit or with the explicit knowledge of the customer
- the *data subject* did not request the erasure of their data and the *data controllers* legitimate interest continues to hold
- there are lawful reasons prescribing the *data processing*, especially but not exclusively such as requirements for invoicing, accounting, and other mandatory file keeping in the context of business and trading operations.

#### 5.3.2.7. Clarification of the rights of the data subjects

The *data subjects* have all rights granted by the applicable law, of which we provide an overview in chapter [9. The rights of the data subjects](#) of this document.

On top of the generic information, the additional information provided below must be taken into account:

**The *data controller* maintains the right to partially or entirely erase the data being processed in the context of the orders and cease such *data processing* at the time of shutting down the operation of the webshop or for any other reason arising on their own behalf without any prior notice to the *data subjects*.**

Since the customer receives all important data produced in the context of the orders in the form of confirmation messages in electronic mails, the *data subject's* own responsibility in storing such data is primary from the perspective of their own. If, the destruction of the data or the cessation of the *data processing* on the *data controllers* behalf causes harm to the interests of the *data subject*, the ***data subjects* admits their exclusive responsibility by accepting the terms of this *Privacy Policy*** considering the fact that it is considered their own negligence if they failed to keep the received confirmation mails.

**The *data subjects* understand that if the *data controller* partly or entirely destroys the data or ceases the *data processing*, the *data controller* is no longer able to fulfil the requests of the (former) *data subjects* with regards of the affected data.**

These however does not affect the *data subjects'* rights in any way as long as the *data processing* is not ceased.

#### 5.3.2.8. Data processors performing data processing

In the the course of the provision of the webshop service the following hosting provider performs *data processing as a data processor*:

##### **GreenGeeks**

Principal address: 5739 Kanan Rd, Suite 300 Agoura Hills, CA 91301 USA

E-mail address: [support@greengeeks.com](mailto:support@greengeeks.com)

#### 5.3.2.9. Information about transfers of personal data to third countries or international organisations

GreenGeeks as a *data processor* serves the visitors and provides the service from their data centre located in the Netherlands, so the *personal data* of the *data subjects* are not transferred directly to *third countries* or *international organisations*.

However GreenGeeks, when it is essential for the provisioning of the service, may access the *processed data* from a third country. GreenGeeks provides the safeguards for the *data controller* and the *data subjects*, that they adhere to the regulations of GDPR as stated below:

- <https://www.greengeeks.com/legal/dpa> - especially under paragraphs 3/H and 3/I

PayPal as a *data controller* serves the payments and provides the service from their data centre located in Luxembourg, so the *personal data* of the *data subjects* are not transferred to *third countries* or *international organisations*.

However PayPal, when it is essential for the provisioning of the service, may access the processed data from a *third country*. PayPal provides the safeguards for the *data subjects*, that they adhere to the regulations of GDPR as stated below:

- <https://www.paypal.com/hu/webapps/mpp/ua/privacy-full#7>

Other providers used during the fulfilment of orders provide as *data controllers* provide the safeguards for the *data subjects*, that they adhere to the regulations of GDPR as stated below:

- Magyar Posta: [https://www.posta.hu/adatkezelesi\\_tajekoztato#2](https://www.posta.hu/adatkezelesi_tajekoztato#2).

## 5.4. Data processing related to customer relationship and other communications

**Attention:** The *data processor* provides their contact details below solely for the purpose of contact and communication related to their business. Slezsák Csilla SP does not consent to the usage of the contact details and communication options provided on the Coconut Design Websites without an explicit permission to be used by others for contacting them regarding subjects not related to their business (especially for the advertising or offering of products or services) or to perform any *data processing* on those details (especially the storage of those details in a database or the forwarding or selling of those details).

### 5.4.1. The fact of the data processing

If someone has questions, remarks or problems related to the services or *data processing* of the *data processor* or the contents of the Coconut Design Websites, they may get in touch with the *data processor* using the contact details and methods published on the website (phone, email, social media sites, postal mail etc.)

The *data processor* performs *data processing* for any mails, electronic messages and information conveyed in writing or over phone together with information unambiguously identifying the source (such as name, email or postal address, phone number) and any other personal information voluntarily provided during the communication.

#### 5.4.2. The range of persons who are data subjects

Those, who get in touch with the *data controller* using any of the contact methods provided on the Coconut Design Websites.

#### 5.4.3. Purposes of the processing

The primary purpose of the *data processing* is to enable the efficient and convenient communication with those who get in touch with the *data controller*. The purpose of the communication may be among others to keep in touch with customers and partners, to negotiate the details of cooperation, maintain communication and relations, answering questions and enquiries, provide information etc.

#### 5.4.4. The legal basis of the data processing

##### 5.4.4.1. Determination of the basis of the data processing

There may be multiple legal bases of the *data processing* during the communication.

Legal basis can be on one hand if the *data subject* gives consent as defined under point (a) of paragraph 1 of Article 6 of GDPR to the *data processing* during getting in touch:

“[Processing shall be lawful [...] if...] the data subject has given consent to the processing of his or her personal data [...]”

This may be true if the *data subject* uses the contact form on the website and marks the checkbox indicating consent for the *data processing*.

However in some cases this kind of explicit prior consent cannot be obtained, for example if the contact request is made to the *data processor* over email or phone. In such cases the legal basis for the *data processing* is the legitimate interest as defined under point (f) of paragraph 1 of Article 6 of GDPR:

“[Processing shall be lawful [...] if...] processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party [...]”

Since in these cases the *personal data* revealed to the *data controller* at the same time as the contact request itself without a chance to obtain prior consent, also since the device used for the communication may also automatically store the data, there is no reasonable and lifelike way to obtain prior consent.

Since as described above the *data processing* under point (a) of paragraph 1 of Article 6 of GDPR cannot happen, and points (b) to (e) do not provide a suitable legal basis either, the *data processing* may only happen according to point (f) as necessary for the purposes of the legitimate interests.

To apply this legal basis the *data controller* should perform a Legitimate Interests Assessment. We provide the steps and the results of that below.

#### 5.4.4.2. Assessment of the legitimacy of the interest behind the data processing

It is a shared interest of both the *data controller* and the *data subjects* to fulfil the goal of the communications in the most efficient way, it is necessary for the *data controller* to know who they are communicating with and what was the history of prior communications.

#### 5.4.4.3. Assessment of the necessity of the data processing

It is common practice for two parties communicating to store and review the communication history, and in some cases quote from or refer back to it. Without that some information was required to be asked and answered again and again, which would make the communication very hard and would create an unrealistic situation, also would hinder or in most cases completely prevent the maintenance of business and customer relations as well as responding to requests and questions. Based on that the *data processing* described in this chapter is absolutely necessary.

#### 5.4.4.4. Assessment of the impact for the data subjects and their interests

The data collected during the *data processing* allows the *data controller* to identify the parties participating in the communication.

On the other hand this does not necessarily means the determination of the real identity of the communicating parties. The *data controller* does not require and does not verify the validity of the data provided during communication. Since the *data controller* can identify the communicating parties within the context of a given communication regardless of their real identity, the *data subjects* may decide to conceal any data they would like to exclude from the *data processing* as they see fit (for example using pseudonyms, throw away email addresses, restriction of caller ID etc.).

Based on that we can conclude that in the context of this *data processing* the providing of the *data subjects* data is always voluntary, therefore the responsibility for any effects arising from the *data processing* is in significant part held by the *data subjects* themselves.

#### 5.4.4.5. The balance between the legitimate interest of the data controller and the protection of the interest of the data subjects

Based on the assessments performed above it can be determined, that the risk of harm to the interests of the *data subjects* is low, the *data subjects* have several ways to reduce their own risks and the widely adopted practices also suggest that the *data controller* is reasonable to assume the legitimate interest as the basis of the *data handling* as defined under point (f) of paragraph 1 of Article 6 of GDPR during the communication.

Since it is common practice for the communicating parties to store and keep mails, messages, addressing information enabling the two way communication and the contents of the information communicated, it is a reasonable expectation on the *data subjects* behalf that they become subject of such *data processing* in the context of communication discussed in this chapter. Based on that obtaining a previous consent for or providing prior information would not only be impossible or unrealistic as described previously, but may also be unreasonable and unnecessary, more over annoying and unpleasant provided that the data subject has reasonable knowledge about the common norms of bi-directional communication.

The *data processor* draws the attention of the *data subjects* to that they may exercise their rights during or after the communication to restrict or forbid the *processing* of their *personal data* for the *data processor*.

#### 5.4.5. List of recipients and those entitled to access the data

The data obtained during the *data processing* is not accessible for the *data subjects*, only for the *data controller*. The *data controller* respecting the stated principles prevents the access to the data without a sufficient cause.

The *data controller* may hand over the data being processed to the appropriate authorities in case of suspected criminal offences, cyber-attacks or in case of any other cases if required by the applicable law.

Apart from that there are no recipients of the data stored, i.e. the *data controller* does not disclose the stored data to anyone else.

#### 5.4.6. Time-frame of the data handling

The time-frame of the data processing may vary based on the legal basis as follows:

- In the cases, when the legal basis for the data processing is the legitimate interest as defined under point (f) of paragraph 1 of Article 6 of GDPR, the duration of the *data processing* is the duration for which the legitimate interest continues to hold. In practice this means that the *data controller* may *process* the data made available to them as long as it is potentially helpful for present or future communications. So the time-frame of the data handling lasts until:
  - the *data subject* requests the erasure of their *personal data* as described in Article 17 of GDPR (or more precisely until such request is fulfilled by the *data controller*),  
or
  - the cessation of the interests of the *data controller* (except for the case if the *data subject* has requested the restriction of the *data processing* as described in Article 18 of GDPR including or explicitly restricting the erasure of such data)or until the one that happens sooner of these.
- In the cases, when the legal basis of the *data processing* is the consent of the *data subject* as defined under point (a) of paragraph 1 of Article 6 of GDPR the time-frame of the *data processing* lasts until:
  - the *data subject* revokes their consent, or
  - the *data subject* requests the erasure of their *personal data* as described in Article 17 of GDPR (or more precisely until such request is fulfilled by the *data controller*),  
or
  - the cessation of the interests of the *data controller* (except for the case if the *data subject* has requested the restriction of the *data processing* as described in Article 18 of GDPR including or explicitly restricting the erasure of such data)or until the one that happens the soonest of these.

If the data is transmitted to public authorities in case of suspected criminal offences or cyber-attacks, any further *data processing* is going to be performed and decided about by those bodies acting within their own competence, and the *data controller* cannot be held responsible for the details of the further *processing* of the data. In such cases the time at which the data is deleted or the way the data is *processed* cannot be guaranteed within the context of this document.

### 5.4.7. Clarification of the rights of the data subjects

The *data subjects* have all rights granted by the applicable law, of which we provide an overview in chapter [9. The rights of the data subjects](#) of this document.

### 5.4.8. Data processors performing data processing

#### 5.4.8.1. Email

During email communication or during the operation of the contact forms on the website the following service provider as a *data processor* participates in the *data processing* by providing the required infrastructure:

##### **GreenGeeks**

Principal address: 5739 Kanan Rd, Suite 300 Agoura Hills, CA 91301 USA

E-mail address: [support@greengeeks.com](mailto:support@greengeeks.com)

##### **Google Ireland Limited**

Principal address: Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland

Location: [https://support.google.com/policies?p=privpol\\_privts](https://support.google.com/policies?p=privpol_privts)

Data processing information: <https://policies.google.com/privacy>

#### 5.4.8.2. Facebook Messenger

The below service provider participates in double quality when communicating using Facebook messages:

- on one hand as a *data processor* as the provider of the infrastructure required for the communication described in this chapter,
- on the other hand as *data controller* as the provider of the Facebook service.

So the persons communicating over Facebook does not only become *data subjects* in the context of the *data processing* performed by Slezsák Csilla SP as the *data controller* as described in this chapter, but they also become *data subjects* to the *data processing* performed by Facebook as *data controller* as the provider of the Facebook service. Details of the organisation acting as both *data controller* and *data processor* are the following:

##### **Facebook Ireland Limited**

Principal address: 4 Grand Canal Square, Grand Canal Harbour, Dublin, D02, Ireland

Location: <https://www.facebook.com/privacy/explanation> (bottom of the page)

Data processing information: <https://www.facebook.com/privacy/explanation>

Data processing terms: <https://www.facebook.com/legal/terms/dataprocessing>

#### 5.4.8.3. Other services

The *data controller* draws the attention of the *data subjects* to that similarly to those described above regarding Facebook, most likely they may also become *data subjects* in the context of the providers of the communication infrastructure as *data controllers* when using any other means of electronic communication services for the purpose of getting in touch or communicating, additionally to becoming *data subjects* of the *data processing* performed by Slezsák Csilla SP as the *data controller*. Regarding the details of such, please, always obtain information from the operator of the given service or system, because such *data processing* is independent of this *Privacy Policy* and the *data processing* performed by Slezsák Csilla SP.

#### 5.4.9. Information about transfers of personal data to third countries or international organisations

GreenGeeks as a *data processor* serves the visitors and provides the service from their data centre located in the Netherlands, so the *personal data* of the *data subjects* are not transferred directly to *third countries* or *international organisations*.

However GreenGeeks, when it is essential for the provisioning of the service, may access the processed data from a *third country*. GreenGeeks provides the safeguards for the *data controller* and the *data subjects*, that they adhere to the regulations of GDPR as stated below:

- <https://www.greengeeks.com/legal/dpa> - especially under paragraphs 3/H and 3/I

Google and Facebook provide their services within the European Union through their subsidiaries located in Ireland, so the *personal data* of the *data subjects* are not transferred directly to *third countries* or *international organisations*. At the same time the attention of *data subjects* is drawn to the fact that these organisations provide the safeguards for the *data controller* and the *data subjects* to not transfer the *personal data* of the *data subjects* to *third countries* or *international organisations* as stated below:

- Facebook: <https://www.facebook.com/about/privacysshield>
- Google: <https://policies.google.com/privacy/frameworks>

On top of that, similarly to those described at the end of the last subtitle, it is possible that the data of the *data subject* in the context of the communication infrastructure or system is forwarded to a *third country* or an *international organisation* independently from this *Privacy Policy* and the *data processing* performed by Slezsák Csilla SP. Regarding the details of such, please, always obtain information from the operator of the given service or system!

### 5.5. Data processing related to the newsletter service

Slezsák Csilla SP as the provider of the Coconut Design Websites operates an electronic (email based) newsletter service for those interested. Anyone may subscribe to the said newsletter considering the terms described here, who has an email address that can receive the newsletter and who gives consent to the data processing required for the operation of the newsletter service.

The newsletter is written to primarily contain information about the contents of the Coconut Design Websites, news, changes related to Coconut Design as well as about products and promotions. The newsletter may contain offers to sell products or services! In some cases the newsletter may contain information and offers related to the business partners of Coconut Design, non-profit organisations supported by Coconut Design, as well as news, spectacles and calls to action as long as these are consistent with the mentality of Coconut Design.

The newsletter is always sent by the data controller. Data processors are being used during the sending of emails, however the right to send such email always remains with the data controller. Such right as well as the information of the subscribers is never given to 3rd parties.

For the operation of the newsletter service Slezsák Csilla SP – as the *data controller* with the previously declared contact details – performs *data processing* regarding the subscribers, of which details are provided below.



### 5.5.1. The fact of the data processing

The prerequisite for the consumption of the newsletter service is the subscription, and the prerequisite of the subscription is the providing of the personal details required for the delivery of the newsletter and the giving of the required consent for the *data processing*. Without a consent the *data controller* has no legal basis for the processing of the data required for the delivery of the newsletter, so the service cannot be provided.

The **email address of the subscriber (*data subject*)** is necessary for the delivery of the newsletter.

On top of that, in order for the *data controller* to be able to prove that the subscriber has given consent for the *data processing*, **the name of the *data subject*** is also required.

Slezsák Csilla SP maintains a register of the subscribers in order to provide the newsletter service.

This register contains the following information:

- The email address of the subscriber: required for the delivery of the newsletter.
- Name of the subscriber: required for the *data processing* consent.
- The fact of the *data processing* consent.
- The way the consent has been acquired (e.g. at an event, online etc.)
- The date of obtaining the *data processing* consent.

Slezsák Csilla SP does not process any other *personal data* in relation to the newsletter service.

### 5.5.2. The range of persons who are data subjects

Those, who has explicitly subscribed to the newsletter service on the Coconut Design Websites or other ways (e.g. at an event) and has given consent for the *data processing*.

### 5.5.3. Purposes of the processing

The purpose of the register is twofold:

- enables the delivery of the emails to the right recipients, and
- contains the consent given by the subscribers to Slezsák Csilla SP for the *data processing* required for the newsletter.

#### 5.5.3.1. The legal basis of the data processing

The legal basis of the *data processing* is the consent of the *data subject* as defined under point (a) of paragraph 1 of Article 6 of GDPR:

“[Processing shall be lawful [...] if...] the data subject has given consent to the processing of his or her personal data [...]”

#### 5.5.3.2. List of recipients and those entitled to access the data

The *personal data* may be obtained by the following, while respecting the principles expressed here:

- the co-workers and representatives of the *data processor*, who must for providing the newsletter service, and
- the co-workers responsible for the *data processing*, such as administrators and the data protection officer, if it is required for their activities as long as those are consistent with the goals of the organisation.

There are no recipients of the data, i.e. the *data controller* and the *data processor* does not disclose this data to anyone else.

#### 5.5.3.3. Time-frame of the data handling

The *data controller* processes the data related to the newsletter service, until the *data subject* revokes their consent or until the fulfilment or cessation of the goals associated with their maintenance (e.g. until the end of the availability of the newsletter service).

#### 5.5.3.4. Clarification of the rights of the data subjects

The *data subjects* have all rights granted by the applicable law, of which we provide an overview in chapter [9. The rights of the data subjects](#) of this document.

On top of the generic information, the *data controller* highlights the below details:

**The *data controller* does not send unsolicited advertisement emails to the subscribers of the newsletter service.**

Any subscriber of the newsletter service may unsubscribe from the service without providing any justification and free of charge. In that case the *data controller* erases all information about the *data subject* that was obtained in the context of the newsletter service and does not send newsletter any more to the *data subject* (provided they do not subscribe again).

Unsubscribe from the newsletter can be done by sending an email to the [csilla@coconutdesign.eu](mailto:csilla@coconutdesign.eu) address or by clicking on the unsubscribe link<sup>9</sup> in the newsletter (if it contains such).

Please take into account, that in order to minimise abuse, we can only fulfil requests for the modification of data including unsubscribing requests, if it directly comes from the email address used for the subscription, or if the identity matching those of the subscriber or the right to act on behalf of the subscriber is proven beyond question in other ways.

#### 5.5.4. Data processors performing data processing

During operation of the subscription form on the website, the maintenance of the subscriber register or during the transmission of the emails the following service provider as a *data processor* participates in the *data processing* by providing the required infrastructure:

##### **GreenGeeks**

Principal address: 5739 Kanan Rd, Suite 300 Agoura Hills, CA 91301 USA

E-mail address: [support@greengeeks.com](mailto:support@greengeeks.com)

During the transmission of the emails the following service provider *data processor* participates in the data processing by providing the required infrastructure:

##### **Google Ireland Limited**

Principal address: Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland

Contact details: [https://support.google.com/policies?p=privpol\\_privts](https://support.google.com/policies?p=privpol_privts)

Data processing terms: [https://gsuite.google.com/terms/dpa\\_terms.html](https://gsuite.google.com/terms/dpa_terms.html)

---

<sup>9</sup> It may happen due to technical reasons that the email does not contain an unsubscribe link.

## Mailchimp

Principal address: 675 Ponce De Leon Ave NE #5000, Atlanta, USA

Contact details: <https://mailchimp.com/contact/>

Data processing terms: <https://mailchimp.com/gdpr/>

## MailerLite

Principal address: Ground Floor, 71, 2 Baggot Street Lower, Dublin, D02 P593, Ireland

Contact details: <https://www.mailerlite.com/contact-us>

Data processing terms: <https://www.mailerlite.com/gdpr-compliance>

The *data controller* draws the attention of the *data subjects* to that most likely they also become *data subjects* in the context of the providers of the communication infrastructure as *data controllers* when using means of electronic mailing services (for example to receive the newsletter emails), additionally to becoming *data subjects* of the *data processing* performed by Slezsák Csilla SP as the *data controller*. Regarding the details of such, please, always obtain information from the operator of the given service or system, because such *data processing* is independent of this *Privacy Policy* and the *data processing* performed by Slezsák Csilla SP.

### 5.5.5. Information about transfers of personal data to third countries or international organisations

GreenGeeks as a *data processor* serves the visitors and provides the service from their data centre located in the Netherlands, so the *personal data* of the *data subjects* are not transferred directly to *third countries* or *international organisations*.

However GreenGeeks, when it is essential for the provisioning of the service, may access the processed data from a *third country*. GreenGeeks provides the safeguards for the *data controller* and the *data subjects*, that they adhere to the regulations of GDPR as stated below:

- <https://www.greengeeks.com/legal/dpa> - especially under paragraphs 3/H and 3/I

Google provides their services within the European Union through their subsidiaries located in Ireland, so the *personal data* of the *data subjects* are not transferred directly to *third countries* or *international organisations*. At the same time the attention of *data subjects* is drawn to the fact that this organisation provide the safeguards for the *data controller* and the *data subjects* to not transfer the *personal data* of the *data subjects* to *third countries* or *international organisations* as stated below:

- <https://policies.google.com/privacy/frameworks>

Mailchimp provides their services as an operation based in the USA, therefore the *personal data* of the *data subjects* are not transferred directly to *third countries* or *international organisations*.

During the *processing* the *data processor* provides safeguards for the privacy of the *data subjects* for the *data controller* and the *data subjects* as stated below:

- <https://mailchimp.com/help/mailchimp-european-data-transfers/>

MailerLite provides their services within the European Union through their subsidiaries located in Ireland, however the *personal data* of the *data subjects* may still be transferred directly to *third countries* or *international organisations*. At the same time the attention of *data subjects* is drawn to the fact that this organisation provide the safeguards for the *data controller* and the *data subjects*

to not transfer the *personal data* of the *data subjects* to *third countries* or *international organisations* as stated below:

- <https://www.mailerlite.com/legal/data-processing-agreement> – especially section 13

On top of that, similarly to those described at the end of the last subtitle, it is possible that the data of the *data subject* in the context of the communication infrastructure or system is forwarded to a *third country* or an *international organisation* independently from this *Privacy Policy* and the *data processing* performed by Slezsák Csilla SP. Regarding the details of such, please, always obtain information from the operator of the given service or system!

Moreover, during the transmission of the email newsletters based on the nature of the works of email messages, it is possible that the emails are reaching your inbox through the infrastructure of other providers, therefore it is possible that in the context of the communication infrastructure or system the emails are forwarded to a *third country* or an *international organisation* independently from this *Privacy Policy* and the *data processing* performed by Slezsák Csilla SP.

### 5.5.6. Additional related information

Slezsák Csilla SP does not incur an obligation to provide a newsletter service. Subscription and giving consent does not create an obligation for the *data controller* to provide a newsletter service.

## 5.6. Additional data processing

The *data controller* provides details of any *data processing* not covered in the *Privacy Policy* at a time and in a way described in chapter [4. Legal background](#).

## 6. Data transfers

On top of the cases described under each *data processing* the *data controller* may also be lawfully required to provide information, disclose and hand over data and documents in case of exceptional requests by public authorities or other organisations if granted by the applicable law.

In such cases the *data controller* only conveys a measure and quantity of *personal data* to the extent it is absolutely necessary for the goal of such request, provided that the goal and the range of the *requested data* has been defined.

## 7. Data processing principles

The *data controller* designs and implements the *data processing* operations in a way, to ensure the protection of the privacy of the *data subjects*.

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the *processing*, the *controller* shall, both at the time of the determination of the means for *processing* and at the time of the *processing* itself, implement appropriate technical and organisational measures, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the *processing* in order to meet the requirements of the applicable regulations and protect the rights of *data subjects*.

The *data controller* shall implement appropriate technical and organisational measures for ensuring that, by default, only *personal data* which are necessary for each specific purpose of the *data processing* are processed.

The *data controller* chooses and operates the information technology devices and services in a way, that the data has:

- **availability of adequate level**, meaning that the data is accessible and the required devices to access are available for those with rights to access it;
- **protected authenticity and credibility**, meaning that the data is safe against unsubstantiated intentional modifications;
- **provable integrity, consistency and correctness**, meaning that the accuracy of the data and the *data processing* is sound and complete and the data is protected from damage, unintended change and destruction;
- guaranteed **confidentiality** and maintained **security**, so it is protected from unauthorised access.

The *data controller* ensures that data stored in separate registers cannot be directly connected to each other or to the *data subjects*, except for the cases when this *Privacy Policy* provides a prior notification of that.

If the *data controller* has grounds to assume that the *processing* (especially the erasure or modification) of the stored data would harm the legitimate interests of the *data subject*, they restrict the further processing of the data (i.e. prevents the erasure or modification by adequate flagging) until the cessation of the relevant interests is proven or reasonably assumable. So the duration of the storage for data restricted in such way may be different from the otherwise declared time-frame when interests as described above hold.

The *data controller* erases the data if

- the data processing is unlawful or becomes unlawful, especially if
  - the data is no longer connected to a goal or the *data processing* is no longer required for the goals, or
  - the duration of *processing* defined in law, international agreement or legally binding acts of the European Union is over, or
  - the *data processing* has lost original legal basis and there is no other legal basis for the *processing*, or
- the data is incomplete or incorrect to such an extent that is incompatible with the goals of the *data processing* and this condition cannot be remedied in a lawful way,
- the *data subject* requests the erasure of the data in a credible way and there are no known interests conflicting with this requests that may enjoy precedence or
- the erasure of the data is required by law, a legal act of the European Union, an authority or a court

provided that the erasure is not forbidden by the law of the European Union or a Member State.

If the *data controller* becomes aware that any data being processed is incorrect, inaccurate or obsolete or does not correspond to a real situation

- corrects the information if data is available that correspond to a real situation, or
- in the lack of correct data, deletes the incorrect data, provided that the processing of it is not restricted.

The *data controller* flags the data, if the *data subject* disputes the correctness or the accuracy of the data, but the incorrect or inaccurate state of the data cannot be determined unequivocally.

The *data controller* shall communicate any rectification or erasure of *personal data* or restriction of *processing* carried out in accordance with Article 16, paragraph 1 of Article 17 and Article 18 of GDPR to each recipient to whom the *personal data* have been disclosed, unless this proves impossible or involves disproportionate effort.

The *data controller* shall maintain a record of *processing* activities under its responsibility in accordance with Article 30 of GDPR to ensure the lawfulness of *processing* and in order to facilitate the provision of information to the *data subjects* in case of a request.

## 8. Security of data

The *data controller* and the delegated *data processors* in accordance with Article 32 of GDPR take appropriate technical and organisational measures to ensure the adequate level of security of data.

The *data controller* and the *data processor* implement measures taking into account the state of the art and the cost of implementation to protect the data, especially from unauthorised

- access,
- alteration,
- disclosure by transmission,
- dissemination,
- erasure or destruction, also from
- accidental destruction or damage, and
- from the loss of access due to the changes in technology.

The *data controller* and the *data processor* implement technical and organisational measures taking into account the state of the art and the cost of implementation to ensure the security of the data processing. The goal of these measures among others is to provide protection from

- information technology fraud,
- spying,
- computer viruses,
- spam,
- hacking,
- and other attacks and abuses.

The *data controller* and the *data processors* additionally shall take steps to ensure that any natural person acting under the authority of the *controller* or the *processor* who has access to *personal data* does not process them except on instructions from the *controller*, in accordance with the principles in this *Privacy Policy*, unless he or she is required to do so by Union or Member State law.

### 8.1. Data breach

In the case of a *personal data breach*, the *data controller* shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the *personal data breach* to

the supervisory authority competent, unless the *personal data breach* is unlikely to result in a risk to the rights and freedoms of natural persons.

When the *personal data breach* is likely to result in a high risk to the rights and freedoms of natural persons, the *data controller* shall communicate the *personal data breach* to the *data subjects* without undue delay, except in the cases described under paragraph 3 of Article 34 of GDPR.

The *data controller* shall document any *personal data breaches* regardless of severity of the risks, comprising the facts relating to the *personal data breach*, its effects and the remedial action taken and all other details required by the law prescribing the *data processing*.

## 9. The rights of data subjects

The *data controller* shall provide information on action taken on a request aimed to exercise the rights described below to the *data subject* without undue delay and in any event within 1 (one) month of receipt of the request. That period may be extended by 2 (two) further months where necessary, taking into account the complexity and number of the requests.

The provisioning of the information is free of charge, but according to paragraph 5 of Article 12 of GDPR

- charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- if the request of the data subject is manifestly unfounded or excessive in character the data controller may refuse to act on the request.

If the *data controller* has reasonable doubts about the identity of the natural (or legal) person behind the request, they may require additional information to confirm the identity of the requester.

If the *data controller* does not take action on the request of the *data subject*, the *controller* shall inform the *data subject* without delay and at the latest within 1 (one) month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

The *data subject* may also exercise their rights assisted by Adatvédelmi és Információszabadság Hatóság (national authority for data protection and freedom of information of Hungary) to amend, erase or restrict the processing of the *personal data processed* by the *data controller* or the *data processors* commissioned or ordered by the *data controller*.

### 9.1. Access right of the data subject (rights of information)

According to Article 15 of GDPR the *data subject* shall have the right to obtain from the *controller* confirmation as to whether or not *personal data* concerning him or her are being *processed*, and, where that is the case, access to the *personal data* and the following information:

- the purposes of the *processing*;
- the categories of *personal data* being processed;
- the recipients or categories of recipient to whom the *personal data* have been or will be disclosed,
- where possible, the envisaged period for which the *personal data* will be stored, or, if not possible, the criteria used to determine that period;

- where the *personal data* are not collected from the *data subject*, any available information as to their source;
- the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the *data subject*;
- where *personal data* are transferred to a *third country* or to an *international organisation*, about the fact of the transfer and the appropriate safeguards pursuant to Article 46 relating to the transfer.

The *data controller* draws the attention of the *data subjects* to that most of this information is provided in detail in this *Privacy Policy* apart from exceptional cases, so before expressing requests for such information it is recommended to thoroughly read and closely examine the contents of this document.

## 9.2. Right to rectification

According to Article 16 of GDPR the *data subject* shall have the right to obtain from the *controller* without undue delay the rectification of inaccurate *personal data* concerning him or her. Taking into account the purposes of the *processing*, the *data subject* shall have the right to have incomplete *personal data* completed, including by means of providing a supplementary statement.

## 9.3. Right to erasure ('right to be forgotten')

The *data subject* shall have the right to obtain from the *controller* the erasure of *personal data* concerning him or her without undue delay and the *controller* shall have the obligation – in accordance with paragraph 2 and 3 of Article 17 of GDPR – to erase *personal data* without undue delay where any of the grounds described under paragraph 1 of Article 17 of GDPR apply, especially if the *data subject* withdraws consent on which the *processing* is based according to point (a) of paragraph 1 of Article 6, or point (a) of paragraph 2 of Article 9, and where there is no other legal ground for the *processing*.

## 9.4. Right to restriction of processing

The *data subject* shall have the right – in accordance with paragraph 2 of Article 18 of GDPR – to obtain from the *controller* restriction of *processing* (i.e. for the *data controller* to flag the data in order to restrict their future processing) where one of the cases described under paragraph 1 of Article 17 of GDPR apply.

One of such possible restrictions may be the restriction of deletion, which may be of particular importance when the *data subject* needs the data being processed related to them for some reason so it is important to prevent their deletion.

## 9.5. Right to data portability

According to paragraph 1 of Article 20 of GDPR the *data subject* shall have the right – in accordance with paragraph 2-4 of Article 20 of GDPR – to receive the *personal data* concerning him or her, which he or she has provided to a *controller*, in a structured, commonly used and machine-readable format and have the right to transmit those data to another *controller* without



hindrance from the *controller* to which the *personal data* have been provided, if the the *processing* is based on consent or on a contract and the *processing* is carried out by automated means.

## 9.6. Right to object

The *data subject* shall have the right to object, on grounds relating to his or her particular situation, at any time to the *processing of personal data* concerning him or her as described in Article 21 of GDPR if

- The legal basis of the *data processing* is point (e) or (f) of paragraph 1 of Article 6 of GDPR, or if the *personal data* are processed for
- direct marketing purposes, or
- scientific or historical research purposes or statistical purposes, or
- other purposes providing a legal bases for the objection of the *data subject*.

The *data controller* declares that point (e) of paragraph 1 of Article 6 of GDPR is not used as the legal basis for any of the *data processing* performed, and that legitimate interest as defined under point (f) of paragraph 1 of Article 6 of GDPR is only used as the legal basis fro the *data processing* in the cases described in this *Privacy Policy*.

If the *data controller* determines the rightfulness of the objection of the *data subject*, they cease the *data processing* – including the recording and transfer – and lock the data, and notify everyone about the objection and the actions taken whom the data has been transferred to or who must act for the enforcement of the right to object.

## 9.7. Right to the protection from automated decision-making

According to paragraph Article 22 of GDPR the *data subject* shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

# 10. Legal remedies

## 10.1. Complaint

According to point (f) of paragraph 1 of Article 15 of GDPR the *data controller* hereby inform the *data subjects* about their right to submit their complaints to supervisory authorities.

Complaints against the potentially unlawful conduct of the *data controller* may be submitted to Adatvédelmi és Információszabadság Hatóság (national authority for data protection and freedom of information of Hungary):

**Nemzeti Adatvédelmi és Információszabadság Hatóság (national authority for data protection and freedom of information of Hungary)**

HUNGARY, 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Postal address: 1530 Budapest, Postafiók: 5.

Phone: +36 -1-391-1400

Fax: +36 - 1- 391- 1410

E-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

## 10.2. Judicial enforcement

The ***data subject*** may initiate legal proceedings against the *data controller* or – regarding the *data processing* in the context of the area of activity of the *data controller* – the *data processors*, if they think that the *data controller* or the *data processors* as commissioned or ordered by the *data controller*

- process the *personal data* of the *data subject* in violation of the law or the legally binding acts of the European Union concerned with the *data processing*, or
- request of the *data subject* aimed to exercise their rights is not fulfilled in a timely manner or in an adequate quality.

The *data controller* and the *data processors* bear the burden of proof that the *data processing* is legal under the law or the legally binding acts of the European Union.

The settlement of complaints in a lawsuit is the responsibility of the court. The lawsuit can be filled at the court local to the home address or the place of residence of the *data subject* according to his or her choice.

In a lawsuit even parties without a legal capacity may have standing before the Court. Public authorities may intervene with the lawsuit to enable the succeeds of the *data subject*.

If the court upholds the action it establishes the fact of the infringements and may require the *data controller* and the *data processors*

- to cease the unlawful *data processing*,
- to restore the lawfulness of the *data processing*, and
- may require them to undertake specific course of action to ensure justice for the *data subject*.

## 10.3. Financial responsibility

If the court upholds the action it establishes the fact of the infringements and may require the *data controller* and the *data processors* to pay compensation for material and immaterial damages.

### 10.3.1. Compensation for material damages

If the *data controller*, or the *data processors* as commissioned or ordered by the *data controller* infringe the regulations stated in law or the legally binding acts of the European Union regarding the *processing of personal data* and causes damages to others, those must be reimbursed.

### 10.3.2. Compensation for immaterial damages

If the *data controller*, or the *data processors* as commissioned or ordered by the *data controller* infringe the regulations stated in law or the legally binding acts of the European Union regarding the *processing of personal data* and violates the human rights of a person, the person adversely affected may demand compensation from the *data controller* or the *data processors*.

### 10.3.3. Exemption

The *data controller* is exempt from the responsibility for the damages and from paying compensation if able to prove that the damages or violations to the human rights happened due to reasons outside of the context of the *data processing*.

The *data processor* is exempt from the responsibility for the damages and from paying compensation if able to prove that during the *data processing* performed by themselves they complied with the instructions given in law and the legally binding acts of the European Union regarding the *processing of personal data* and they were compliant with the instructions given by the *data controller* as well.

The damages may be excluded from reimbursement and compensation if the damages or the violations to the human rights of a person are a result of the negligent behaviour of the damaged or the person suffered the violations to the human rights respectively.

## 11. Afterword

The primary purpose of this document is to meet the legal obligations of the *data controller* prescribed by law to provide information for the *data subjects*. Slezsák Csilla SP assumes the responsibility for the information provided in this document fully meet those legal requirements.

In order to facilitate the understanding of this document, on top of that it also provides an overview of some of the legislations relevant for *data processing*. This document however does not provide a complete reference of the legislations related to *data processing* and knowing the contents of it does not substitute the knowing of the legislations themselves. The exact rules are always defined by the regulations in the actual, applicable law and the legally binding acts of the European Union!

During the writing of this document we have consulted the following legislations, recommendations and standards:

- Regulation (EU) 2016/679 of the European Parliament and the Council relating to the protection of natural persons with regard to the *processing of personal data* and rules relating to the free movement of *personal data* (General Data Protection Regulation, GDPR)
- Law CXII of 2011 on the right to self-determination as regards information and freedom of information of Hungary (2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Info law))
- Law CVIII of 2001 on Electronic Commerce and on Information Society Services of Hungary (2001. évi CVIII. törvény – az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről) (especially paragraph 13/A)
- Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers of Hungary (2008. évi XLVII. törvény – a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról)
- Act XLVIII of 2008 on Business Advertising Activity of Hungary (2008. évi XLVIII. törvény – a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól) (especially paragraph 6)
- Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising

- Opinion 06/2014<sup>10</sup> published by the Data Protection Working Party<sup>11</sup> set up under Article 29 of the Data Protection Directive<sup>12</sup>, and the NAIH/2016/1684/2/V resolution based on that published by the Nemzeti Adatvédelmi és Információszabadság Hatóság (national authority for data protection and freedom of information of Hungary) containing fundamental principles regarding the conduct of a Legitimate Interests Assessment in order to use point (f) of paragraph 1 of Article 6 of GDPR as the legal basis for data processing
- RFC 6265 recommendation about the state management over HTTP protocol using cookies

---

<sup>10</sup> [Opinion 6/2014 about the definition of legitimate interest of the data controller as discussed in article 7 of direction 95/46/EC, WP217](#)

<sup>11</sup> The Data Protection Working Party was an independent European working party that dealt with issues relating to the protection of privacy and personal data.

<sup>12</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.