# IEECP personal data privacy, security and protection policy

| |
|---|
| **Version: 1** |
| **Date of version:** May 2021 |
| **Created by:** Mia Dragović Matosović, Jen Heemann, Ivana Rogulj, Marine Perrio, George Stravodimos |
| **Approved by: Vlasios Oikonomou** |
| **Confidentiality level:** This document is visible to all current employees of IEECP who have access to the IEECP team on SharePoint. The document can be edited only by the officially appointed GDPR team members, while others should only make comments or track changes. |

## *Change history*

| Date | Version | Created by | Description of change |
|---|---|---|---|
| November 2020 | 0.1 | Mia Dragović Matosović | Basic document outline |
| February 2021 | 0.1 | Mia Dragović Matosović | Draft of first version of the policy |
| April 2021 | 0.2 | Mia Dragović Matosović | High draft of first version of the policy |
| May 2021 | 0.2 | Vlasios Oikonomou | Final document for 2021 |

This policy will be changed and adapted yearly. The changes from last year will be described here. It is advised for this policy to be revised once a year. After this revision, the main changes from the last version will be described here.

# Contents





Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

# 1. Purpose, scope and users

IEECP strives to comply with applicable laws and regulations related to personal data protection in the countries in which IEECP operates. We are a non-for-profit organisation, our line of work is consulting, and our aim is providing top quality scientific consulting in sustainability and climate change. In accordance with our caring for the environment and excelling in what we do, we are also considerate of the safety and privacy of data we collect.

Since compliance is necessary by all employees, we have included all employees in the process of creating this document, and its main purpose is to clearly communicate our data protection and security policies and control mechanisms, so that they can be understood and enforced.

Annex 15.2 also gives a summary overview of responsibilities for certain IEECP employee functions.

This document defines the basic principles by which IEECP processes the personal data of its data subjects including beneficiaries of its work, suppliers, business partners, employees, and other individuals, as well as describes our data security policies. The Policy also indicates responsibilities of its employees while processing personal data and contains all documents connected to data privacy and security, either as annexes or as links to separate documents.

The main categories of data subjects for IEECP are:

- As IEECP is an EU consultancy working on numerous EU projects, our main data subjects in form of "customers" are **project stakeholders and communication beneficiaries** (i.e. website visitors, followers on social media, newsletter recipients etc.);
- Our main business partners are our **project partners**;
- Our business clients and contractors include in most cases the **European Commission and the Executive Agency for Small and Medium-sized Enterprises (EASME);**
- Our suppliers include services such as **accounting, legal and IT services;**
- Our employees include full- and part-time **staff**, as well as contracted **experts**.

Although IEECP does not by default manage a lot of personal data, and almost no sensitive data, IEECP does carry the role of both the data "controller" and "processor", as we both determine the purposes and means of processing personal data in various projects, and we also process some personal data on behalf of the outside controller in some cases.

**Due to our size, we agreed not to have a data protection officer, but, instead, putting our managing director Vlasios Oikonomou in charge of delegating all data protection related matters which concern IEECP in general and not the specific projects run by IEECP.** Vlasios Oikonomou is also responsible for making data safety and security decisions for most sensitive matters. Each employee that is also a project coordinator is responsible for ensuring that personal data and data safety and security guidelines mentioned in this document are also followed for that particular project.

Other employees might also act as data controllers or processors for certain projects they manage. Some sections of this document name a position or a person who is responsible for a certain process.



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

If the person or a position is not explicitly named, this means that the managing director is responsible for delegating this activity and making sure that it is accomplished.

This Policy applies to IEECP and its employees conducting services/projects within the European Economic Area (EEA) or processing the personal data of data subjects within EEA.

IEECP is registered in The Netherlands, yet is an institution with international employees, our basis therefore being permanent remote work or teleworking, which is described in section 9.3. In our approach to data safety and security we are also mindful of the flexibility we want our employees to have in using both their personal and company devices for their work and this document considers all specificities of remote working.

The users of this document are all employees, permanent or temporary, and all contractors working on behalf of IEECP.

## 2. Reference documents

In creating this document, we have referred to the following guidelines:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- GDPR implementation Act in The Netherlands "Uitvoeringswet AVG"
- Dutch Data Protection Authority "Autoriteit Persoonsgegevens"
- The IEECP internal handbook which gives an outline of IEECP work and identity guidelines
- The UK guide to GDPR policy
- The Belgian guide to GDPR

This document is based on the guidelines and templates of *Advisera Expert Solutions* and is accompanied with various templates which need to be used in certain cases explained in this document. The templates mentioned in this document are the following:

- Employee Personal Data Protection Policy – described in section 6.3, Data controller inventory
- Data Controller Inventory kept in IEECP's internal GDPR folder, and reported each year in this policy, section 6.3
- Data Protection Impact Assessment Guidelines in IEECP internal Advisera template folder 6
- Data Protection Impact Assessment Register available in our internal folder here
- Breach Notification Procedure – described in section 6.4
- Processor GDPR Compliance Questionnaire – available in the GDPR folder 8 "Third Party Compliance"
- IEECP Privacy and Cookie Policy – added in annex and available publicly on IEECP's website
- Template for a Data Management Plan for specific EU projects – Annex 15.1



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

# 3. Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union's General Data Protection Regulation:

**'Personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**'Sensitive Personal data'** or **'Special category data'** are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

**'Data Controller'** is the natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

**'Data Processor'** is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

**'Processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**'Restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future.

**'Profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

**'Anonymization'** means irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The personal data processing principles do not apply to anonymized data as it is no longer personal data.

**'Pseudonymization'** is 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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. An example of pseudonomization is substituting personally identifiable information (such as an



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

individual's name) with a unique identifier using techniques such as coding or hatching. This means that, with having a code by which the pseudonymisation was made, the data can be re-identified. Pseudonymization reduces, but does not completely eliminate, the ability to link personal data to a data subject. Because pseudonymized data is still personal data, the processing of pseudonymized data should comply with the Personal Data Processing principles.

**'Filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

**'Recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

**'Third party'** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

**'Consent'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

**'Personal data breach'** means 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.

**'Supervisory authority'** means an independent public authority which is established by a Member State pursuant to Article 51 of the EU GDPR.

**'Supervisory authority concerned'** means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;
(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
(c) a complaint has been lodged with that supervisory authority.

**'Cross-border processing'** means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

# 4. Basic principles regarding personal data processing

Article 5(2) of the GDPR stipulates that "*the controller shall be responsible for, and be able to demonstrate, compliance with the principles*. IEECP obliges to follow the basic data protection principles which outline the basic responsibilities for organisations handling personal data and will use them as guidance when collecting all personal data:

4.1. **Lawfulness, fairness and transparency** – we have identified an appropriate lawful basis (or bases) for our processing, and we pledge to continue to do so for every future type of personal data which we will collect. We also pledge not to do anything generally unlawful with personal data. We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified and we pledge not to deceive or mislead people when collecting their personal data. Above all, we are dedicated to open and honest way of conducting business, and we strive to always comply with the transparency obligations of the right to be informed. We do not deceive or mislead people when we collect their personal data.

4.2. **Purpose limitation** - Legitimate purpose exists for collecting personal data. All data we collect will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

4.3. **Data minimization** - Only necessary personal data will be collected and stored.

4.4. **Accuracy** – Collected personal data will be kept accurate and, where necessary, kept up to date.

4.5. **Storage period limitation** – Once the purpose of keeping the data ceases to exist, personal data will be deleted, or will be anonymized and as such kept for future analysis.

4.6. **Integrity and confidentiality** – collected and stored data will be kept confidential, with limited access rights kept to minimum and with our active efforts to provide data security. Collected data can be modified only by assigned and authorized persons.

4.7. **Accountability** – with this policy and all its accompanying documents and procedures, IEECP takes responsibility to comply with the GDPR and sets forth ways to demonstrate our compliance. We also take responsibility to review and update our accountability measures at appropriate intervals and **oblige to review this policy and its accompanying documents at least once per year**. Vlasios Oikonomou, as a person in charge of data protection matters, will delegate this task once per year to a specific employee.

# 5. Building data protection in business activities

**5.1. Notification to data subjects** – as described in section 6.1 of this document.

**5.2. Data subject's choice and consent** – as described in section 6.2 of this document.

**5.3. Collection**

IEECP will strive to collect the least amount of personal data possible. If personal data is collected from a third party, it will be ensured by a certain employee responsible for that third-party that the personal data is collected lawfully.



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

### 5.4. Use, retention and consent

The purposes, methods, storage limitation and retention period of personal data must be consistent with the information contained in the Privacy Notice. IEECP will maintain the accuracy, integrity, confidentiality and relevance of personal data based on the processing purpose. Adequate security mechanisms designed to protect personal data must be used to prevent personal data from being stolen, misused, or abused, and prevent personal data breaches.

| |
|---|
| The person responsible for compliance with the requirements listed in this section and regarding data coming from website, newsletter and analytics third parties is IEECP Communications Manager - Marine Faber. |

Our data retention policy (GDPR Articles 5(1)(e), 13(1), 17, 30) and the retention schedule (Article 30) are described in section 6 and they include:

a) Privacy and cookie policy (GDPR articles 12 and 13) – section 6.1
b) The newsletter privacy notice and the newsletter subscription disclaimer – section 6.1
c) Data Subject Consent Form (GDPR Articles 6(1)(a),7(1), 9(2)) – section 6.2
d) Data Subject Consent Withdrawal Form Article 7(3) – section 6.2
e) Parental consent form – section 6.2

### 5.5. Disclosure to Third Parties

| |
|---|
| Whenever IEECP uses a third-party supplier or business partner to process personal data on its behalf, the employee in charge of the process must ensure that this processor will provide security measures to safeguard personal data that are appropriate to the associated risks, i.e., misuse of personal data, an authorized disclosure of personal data, data breaches, etc. |

For this purpose, the **Processor GDPR Compliance Questionnaire must be used**. It is available in the GDPR folder 8 "Third Party Compliance". IEECP must contractually require the supplier or business partner to provide the same level of data protection. The supplier or business partner must only process personal data to carry out its contractual obligations towards IEECP or towards the project for which the controller is responsible, or upon the instructions of IEECP and not for any other purposes. When IEECP processes personal data jointly with an independent third party, IEECP must explicitly specify its respective responsibilities of and the third party in the relevant contract or any other legal binding document, such as the Supplier Data Processing Agreement (GDPR folder 8). In case these templates are used, they should be adapted to the IEECP stationary or to the concrete project stationary in case the processor is used on a concrete project in which IEECP is responsible for handling data protection.

### 5.6. Cross-Border transfers of personal data

– currently, IEECP is transferring personal data in the situations where employees are living outside European Union (administrative documents) or if the project partners are registered in non-EU countries.

The basis for the transborder data transfer is the legally binding Council of Europe Convention No. 108 on the Protection of Individuals regarding Automatic Processing of Personal Data. All the Associated Countries have signed the Convention. The data is transferred to IEECP but trough secure channels and only for internal use. Adequate safeguards are used. If the data



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

imported is further shared, additional safeguards will be applied, including the signing of a **Data Transfer Agreement**, as required by the European Union and, if required, authorization from the relevant Data Protection Authority. The entity receiving the personal data or IEECP if receiver must comply with the principles of personal data processing set forth in Cross Border Data Transfer Procedure.

**5.7. Rights of access by data subjects –** Each IEECP employee, who is acting as a data controller for a certain project, is responsible to provide data subjects with a reasonable access mechanism to enable them to access their personal data, and must allow them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law. The access mechanism will be further detailed in the Data Subject Access Request Procedure.

- Data Subject Access Request Procedure (GDPR Articles 7(3),15, 16, 17,18, 20, 21, 22)
- Data Subject Access Request Form (GDPR Article 15)
- Data Subject Disclosure Form (GDPR Article 15)

**5.8. Data Portability**

Data Subjects have the right to receive, upon request, a copy of the data they provided to us in a structured format and to transmit those data to another controller, for free. The person responsible for the project in question is responsible to ensure that such requests are processed within one month, are not excessive and do not affect the rights to personal data of other individuals (i.e., the request should not affect other person's rights to privacy).

**5.9. Right to be Forgotten**

Upon request, Data Subjects have the right to obtain from IEECP the erasure of its personal data. When IEECP is acting as a Controller, the person responsible for the project in question must take necessary actions (including technical measures) to inform the third parties who use or process that data to comply with the request.

# 6. Data inventory and fair processing guidelines

Personal data regarding IEECP must only be processed when explicitly authorised by the Managing Director Vlasios Oikonomou, who is the person in charge of data protection matters.

IEECP employees in charge of a certain project must decide whether to perform the Data Protection Impact Assessment for each data processing activity according to the Data Protection Impact Assessment Guidelines. You will find this document in the GDPR folder 6 "Data Protection Impact Assessment" and it should be adapted to the IEECP stationary.



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

The Impact assessment is mandatory any time a new large project is planned, in order to ensure the "protection by design" principle. This means that any time IEECP contemplates a major change in the way its data is handled, such as using new technologies or new work platforms, the Managing Director will appoint someone to perform the DPIA, as described in Advisera template folder 6. Notices to Data Subjects.

At the time of collection or before collecting personal data for any kind of processing activities including but not limited to sharing our free products such as obligations, services, or marketing activities, **the person in IEECP responsible for this certain project or selling service** is responsible to properly inform data subjects of **all the following**: the types of personal data collected, the purposes of the processing, processing methods, the data subjects' rights with respect to their personal data, the retention period, potential international data transfers, if data will be shared with third parties and IEECP's security measures to protect personal data. This information is provided through the Privacy and cookie Notice, with the latest update always available on IEECP's website.

Since IEECP manages different projects with other organisations, it is advisable for each project to have its own privacy policy. However, the IEECP employee responsible for this certain project should ensure that the project privacy policy has all the above-mentioned details. Please check annex 15.1 for a proposed template of an EU project Data Management Plan.

For IEECP website visitors and related statistics, mailing purposes and the list of subscribers, we use the privacy policy published on our website: http://www.ieecp.org/privacy-policy-and-data-protection/. Where personal data is being shared with a third-party, **the employee making the contact must ensure that data subjects have been notified of this through the Privacy and cookie policy,** available where they subscribe to the newsletter and easily accessible when visiting IEECP's website**.**

Where personal data is being transferred to a third country according to Cross Border Data Transfer Policy, the Privacy Notice should reflect this and clearly state to where, and to which entity personal data is being transferred. There is no such transfer in IEECP and it is not expected. In case this will happen for any of the project coordinators, they should consult the GDPR Advisera template 7.1.

Where sensitive personal data is being collected, a person responsible for the project in IEECP must ensure that the Privacy Notice explicitly states the purpose for which this sensitive personal data is being collected.

Please use the templates available under GDPR folder 3 for ideas and tips on making new notices.

**The current notices that IEECP is using are:**

## IEECP privacy and cookie policy

This privacy policy explains, in accordance with the EU General Data Protection Regulation 2019/679, IEECP's digital practices and choices you can make about the collection and use of your information (submitted by you or collected through our website). It explains IEECP's policy regarding the nature, purpose, use and sharing of any personal information collected from website visitors or provided to us.
Please note that IEECP is committed to respect your privacy and protect your personal data, that we will not make personal information available to anyone other than our employees and will never use your personal information for marketing purpose and/or share it with third parties.



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

By visiting and using our website, you give your consent to these privacy policy terms.
This policy was last updated in March 2021. Our privacy policy can be updated if need be and we will add any update on this webpage.

## Information collection and use

The information collected on this website will mainly be used by IEECP for:
- Statistics purposes (monitoring and reporting to our funders)
- To keep visitors informed about IEECP activities (newsletter or events registrations) and
- To improve your navigation on our website (internal monitoring to improve website structure and flow).

We may collect personal data from public sources online in the public domain, whenever your professional activity is directly linked to our working topics: for instance, to fulfil our communication and dissemination activities, we gather contact details of officials from the EU Institutions and Member States, journalists or EU associations.
Web visitors IP address is anonymized and not kept within our analytics tools reporting, except for newsletter registrations, which are nonetheless kept strictly confidential and only accessible to the Data Protection Officer: Vlasis Oikonomou, IEECP.
We will not sell, rent, trade or lease any personal data collected online or offline. All information will be kept strictly confidential unless you give us consent to do otherwise.
We collect and temporarily store specific technical data when you visit our website for web management use or security purposes. This data includes:
- Personal information or data
- Cookies and data use

**Personal information or data**

Personal information or data is information that can, with reasons, be used to directly or indirectly identify you or other individuals, such as: name, personal address, phone number, geolocation data, etc. The categories of data collected depend on how you use IEECP's website. By browsing the site, you confirm that you understand and agree to the use of your personal information/data in accordance with this Privacy Policy. If you require any clarification, please contact our data protection officer.
The IEECP website collects and stores only the information submitted when you subscribe to our newsletter or complete an online form such as event registration, or survey. If we ask you to provide personally-identifiable information (such as your name and email), it will only be used to contact or identify you, and you will be informed about it. We use this data to provide you with information you have requested (newsletter subscription) or providing you with information relevant to your interests (event invitations and targeted communication such as EU projects-related newsletters). These are never commercial and sent only sporadically.
The specific case of surveys and interviews will ensure that you are only contacted if you agreed to by clicking a box or similar approval, or allowing you to choose not be further contacted. We use industry standard practices to review data quality and confirm that your information is updated. We also keep data you voluntarily provide at events (through business cards or registration) in order to keep you informed about other similar events.
We provide newsletter subscribers the opportunity to opt out from our mailing list through an "unsubscribe" button available in all newsletters. They can also write at any time to the Data Officer. Registration to the said newsletter is done through a double opt-in process to ensure data security and informed consent.

**Cookies and data use**

Visiting our website is done anonymously. Except for a restricted use and in a way described in this privacy policy, we do not collect identification data of IEECP's website visitors.
For monitoring purposes, we collect data that your browser sends when you visit our website, used to improve the functionality and usefulness of our website. This data can include your computer's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of IEECP's website you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data.
When you access our website with a mobile device, this data may include information such as type of mobile device you use, mobile device unique ID, IP address of your mobile device, mobile operating system, type of mobile Internet browser you use, unique device identifiers and other diagnostic data.
IEECP's website uses cookies (files with a small amount of data which may include an anonymous unique identifier, used for the technical functioning of a website or for gathering statistics) to track general data about



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

how you "use" our website (length of stay and number of visits for instance). Cookies do not identify an individual user, only the computer used. Cookies record areas of the website visited and for how long. This information allows us to understand how our website is used so we can improve it by focusing on content interesting for our users.
Using cookies will not mean we get access to other information or data from your computer and the data allowed will not be used to track your online activity after you leave our website.
Should you wish not to have cookies stored on your computer, please change your settings asking your web browser to refuse them. Refusing cookies, however, can restrict your use of this website. To visit the website and benefit from all its functions, we recommend you leave cookies switched on.

## Retention and disclosure of data

IEECP only retains your personal information or data for as long as is necessary for the purposes set out in this policy. Raw data logs are retained temporarily as required for security and website management purposes only. If required by law and only under very specific circumstances, IEECP might be obliged to share some data or information.

- To comply with a legal obligation,
- To protect and defend the rights or property of IEECP,
- To prevent or investigate possible wrongdoing in connection with the Services,
- To protect the personal safety of users of the Services or the public,
- To protect against legal liability.

## Your rights

Under European data protection laws, you may exercise the following rights at any time:

- Right for transparency and right to information: we provide notice to all website visitors of how we use Personal Data in our everyday operations at the time of collecting Personal Data, or as soon thereafter as possible. This privacy and cookie policy is published to ensure information and transparency.
- Right to be informed about the purposes of processing your data and the identity of the data controller.
- Right to get confirmation of whether or not your personal data is being processed by us and access the data.
- Right to have it rectified, erased or to request restriction of processing or to object to the processing if applicable.
- Right to object and withdraw consent at any time: for all marketing materials, you can opt-out anytime, and free of charge.
- Right to data portability: based on your specific situation, we provide data subjects with the right to obtain and reuse your data across different services and include transferring of your data to you, another controller or a trusted third party.

**Access, erasure and rectification:**

You may exercise your right to access, erase and rectify any of your personal data at any time. You can request this by contacting our Data protection officer by email or writing to IEECP, Amsterdam Sloterdijk Teleport Towers – Kingsfordweg 151, Amsterdam, 1043GR, The Netherlands.
You also have the right to lodge a complaint with your national Data Protection Authority. You can find the contact details of all national data protection authorities here.
The only exception to these rights is for data which IEECP has a legal obligation to keep on record.

## Service providers or third-party services for analytics and others

We may disclose your information to service providers under contract who help with our business operations (such as, but not limited to, fraud investigations, software development, email delivery, marketing communications, bill collection, payment processing, and site analytics and operations). These third parties are authorized to use your Personal Data only as necessary to provide these services to IEECP, for example, the purposes for which the visitor has submitted the information and for the administration of our system or site and/or other internal, administrative purposes. Personal Data may also be transferred to third party service providers of identity management, website hosting and management, data analysis, data backup, security and storage services.
The third-party Service Providers IEECP mostly uses are to monitor and analyse the use of our websites and send newsletters.



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

We will only transfer your Personal Data to any third-party suppliers if and to the extent we are permitted to do so by law or if you have provided your prior consent.

**Newsletter**

If you have subscribed to IEECP email newsletters you will be sent (via email) newsletters, updates and targeted invitations to events related to our work. We will only send this information occasionally and you will have the opportunity to opt-out of these email communications at any time.

The registration is done via a double opt-in procedure: after entering your information on our website, you will receive an email where you should click to confirm your subscription.

Our mailing system is Mailpoet, a GDPR-compliant system. You can access on this page their Data Processing Agreement, privacy policy and contact them.

When you submit a newsletter subscription form, the information you provide will be transferred to IEECP's distribution list for processing in accordance with Mailpoet and IEECP privacy policy and terms.

**Analytics**

We use Google Analytics, a web analytics service offered by Google that tracks and reports website traffic. For information on the privacy practices of Google, please visit the Google Privacy Terms web page.

**Social media**

When interacting on IEECP's social media accounts (Twitter, LinkedIn, Facebook and YouTube), your personal data consent and use are covered by the terms and conditions of the relevant social media platforms.

**Links to Third-Party Sites**

IEECP's Data Privacy Policy applies only to IEECP's website. When you land on external websites or platforms of third parties, even by way of links provided on IEECP's channels, IEECP's data privacy policy ceases to apply.

**Children's Privacy**

Our website does not address anyone under the age of 18 ("Children").

We do not knowingly collect personally identifiable information from anyone under the age of 18. If you are a parent or guardian and you are aware that your Child has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from Children without verification of parental consent, we will take steps to remove that information from our servers.

## Legal notices

**Copyright / intellectual property**

All content on this website, including, but not limited to, graphics, images, texts, videos, animations, sounds, logos, GIFs and icons as well as their formatting are the exclusive property of IEECP, with the exception of trademarks, logos or contents belonging to other partner companies or authors and identified as such.

Any reproduction, distribution, modification, adaptation, retransmission or publication, even partial, of these elements should at least acknowledge the source – IEECP or the project – or look for the express written consent of IEECP. You can do so by emailing IEECP's communication manager, Marine Perrio.

**Information and exclusion**

IEECP uses all the means at its disposal to ensure its website contains reliable, updated and reliable information. However, errors or omissions may occur and, if you find such a deficiency, error or what appears to be a malfunction, please report it to us, describing the problem as precisely as possible (page posing the problem, the triggering action, the type of hardware or browser used, etc.) by emailing IEECP's communication manager, Marine Perrio.

**Contact us**

The controller of your personal data, under applicable data privacy legislation and in regard to the processing of personal information, is:

IEECP – The Institute for European Energy and Climate Policy

Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, Amsterdam, 1043GR, The Netherlands.

Email: info@ieecp.org

IEECP is a foundation, with a registered office at Kingsfordweg 151, 1043GR, Amsterdam, The Netherlands, registered in the Dutch Commercial Register of the Chamber of Commerce under number 64602214.

## The newsletter privacy notice

By subscribing to our newsletter, you give IEECP the consent to collect and process your data according to our Privacy Policy. We will include your e-mail in our mailing list to keep you updated about the IEECP projects and results, no more than once a month.

To this end, the information you are providing will be stored and processed in accordance with the EU GDPR regulation.

The IEECP team is committed to protecting your data. We will keep it strictly confidential, with information access limited to partners and individuals working directly on our projects as well as the European Commission, only for the purpose of providing this service.

## Newsletter subscription disclaimer

By clicking on subscribe, you give IEECP the consent to collect and process your data according to our Privacy Policy. We will include your e-mail in our mailing list to keep you updated about the IEECP projects and results, always in accordance with the EU GDPR regulation and no more than once a month.

## Registry of privacy notices

| **Processing activity** | **Notice type** | **How is the notice presented to users?** | **When is the notice presented to users?** | **Date of last update of notice** | **Location of notice** |
|---|---|---|---|---|---|
| Visiting IEECP website | Website notice | As a pop-up to inform about cookies / tracking and linking to the Privacy policy | When landing on IEECP website | March 2021 | http://www.ieecp.org/privacy-policy-and-data-protection/ |
| Collection of emails for mailing list | Website notice | As a webpage and in the email that is received after subscription | Prior to collection of data | March 2021 | http://www.ieecp.org/newsletters/ and http://www.ieecp.org/privacy-policy-and-data-protection/ |
| Newsletter subscription disclaimer | Website notice | As a webpage and in the email that is received after subscription | Prior to collection of data | March 2021 | http://www.ieecp.org/newsletters/ and http://www.ieecp.org/privacy-policy-and-data-protection/ |
| Legal notices | IEECP legal notices | As a webpage | Available at all times at website footer in the privacy policy | March 2021 | http://www.ieecp.org/privacy-policy-and-data-protection/ |



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

## 6.1. Obtaining consents

Whenever personal data processing is based on the data subject's consent, or other lawful grounds, the person collecting the documents is responsible for retaining a record of such consent in the above registry. In the case of IEECP newsletter and IEECP general communication this is the responsibility of the Communications Manager Marine Perrio, while in the case of particular projects, the main coordinator or person responsible for the project carries this responsibility. The responsible person is also responsible for providing data subjects with options to provide the consent and must inform and ensure that their consent (whenever consent is used as the lawful ground for processing) can be withdrawn at any time.

Where collection of personal data relates to a child under the age of 16, the person responsible for collecting the information must ensure that parental consent is given prior to the collection using a Parental Consent Form, available in this section.

When requests to correct, amend or destroy personal data records, the person responsible must ensure that these requests are handled within a reasonable time frame. The person responsible must also record the requests and keep a log of these in the designated folder here.

Personal data must only be processed for the purpose for which they were originally collected. In the event that IEECP wants to process collected personal data for another purpose, IEECP must seek the consent of its data subjects in clear and concise writing. Any such request should include the original purpose for which data was collected, and also the new, or additional, purpose(s). The request must also include the reason for the change in purpose(s).

As mentioned, the Communications Manager Marine Perrio is responsible for complying with the rules in this section when they regard general IEECP communication, while in the case of particular projects, the main coordinator or person responsible for the project carries this responsibility.

Now and in the future, the responsible person must ensure that collection methods are compliant with relevant law, good practices, and industry standards; and must create and maintain a Register of the Privacy Notices.

### Informed Consent Form

***Note**: The Informed Consent From must be adjusted according to the data collection activity by the person responsible for collecting the data. It must always be accompanied by an Information Sheet, which provides clear and detailed information about the project/activity.*

**I confirm that I understand that by ticking each box below I am consenting to this element of the study. I understand that it will be assumed that unticked boxes mean that I DO NOT consent to that part of the study. I understand that by not giving consent for any one element, I may be deemed ineligible for participating in this project's activity.**

| | |
|---|---|
| I confirm that I have been given a full **explanation of the purpose** of the project's activity. I have read and understood the Information Sheet which I was provided with or listened to an explanation about the project by (responsible person/organisation). | ☐ |



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

| | |
|---|---|
| I have had an opportunity to **consider** what information will be expected of me. I have also had the opportunity to ask questions which have been answered to my satisfaction. | ☐ |
| I agree to appear in **pictures/videos** that may be taken during the activity as evidence of the activity itself and as possible promotional material for the (name of project) project. I understand that these pictures will not be provided to any organisations for commercial purposes. However, they may be processed by third parties as a consequence of their dissemination at international level through the project's social media and website. I understand that the consortium has no control on the images after dissemination. | ☐ |
| I agree that my **anonymised research data** may be used by others for future research (I will not be identifiable when this data is shared). | ☐ |
| I understand that my **participation is voluntary** and that I am **free to withdraw** at any time without giving a reason, and that any data after the time of which it is withdrawn will be no longer be included as part of any future reports, unless I agree otherwise. | ☐ |
| I understand that my personal data will be held and processed in confidence and in accordance with the principles laid out by **GDPR**. | ☐ |
| I am aware of whom I should contact if I wish to lodge a complaint. | ☐ |
| I confirm that I have read and understood the above and freely consent to participate in this project's activity. I have been given adequate time to consider my participation. | ☐ |

**Future activities**

If you would like your contact details to be retained so that you can be contacted in the future by the project researchers who would like to invite you to participate in **further activities of this project**, or in future studies of a similar nature, please tick the appropriate box below.

| | |
|---|---|
| Yes, I would be happy to be contacted in this way* | ☐ |
| No, I would not like to be contacted | ☐ |

**Contact details**

**Name, Surname of participant:** .....

**E-mail (optional):** .....

**Date:** .....

**Signature:** .....



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

## Consent withdrawal form

I, [data subject name and surname], withdraw my consent to process my personal data fort he _____ project. _____ project no longer has my consent to process my personal data for the purpose of [specify legitimate reason of processing personal data], which was previously granted.

**Signature**: .....

**Date**: .....

Once completed, this form should be submitted via e-mail, using the following contact details:

***Note:*** *Contact details of the responsible for conducting the activity should always be provided below. The following table serves as an example.*

| | |
|---|---|
| **Organisation:** | Institute for European Energy and Climate Policy (IEECP) |
| **Contact person:** | Vlasios Oikonomou |
| **Phone:** | +31 70 2500 642 |
| **Email:** | info@ieecp.org |
| **Address:** | Amsterdam Sloterdijk Teleport Towers Kingsfordweg 151, Amsterdam, 1043GR, Netherlands |
| **Website:** | www.ieecp.org |

## Parental Consent form

In view of the GDPR on information security and privacy, we would like to inform you first of all that we will not give your child's data provided to us to other parties.

In addition, we ask explicit permission for a number of specific items. For this purpose, please clearly indicate your choice below. For children under 16 years of age, you must give your parental consent to these data processes.

You can withdraw your consent at any time (Art. 7.3 AVG) by sending an email to _____. The withdrawal of consent is not retroactive.

| | **YES** | **NO** |
|---|---|---|
| May we take group photos during activities and provide them (via mail) to the parents of the children in the group? (If a child does not give permission, we will not distribute the photos). | O | O |
| May we publish photos of activities - on which your child is identifiable - on our website, to illustrate the mention of our pathways and our operation? | O | O |

| | | |
|---|---|---|
| May we publish photos of activities - on which your child is identifiable - on our social media (facebook, linkedin) to illustrate our activities and announcements? | O | O |
| May we publish photos of activities - on which your child is identifiable - in our newsletter, to illustrate the report on our activities? | O | O |
| May local press publish photos of activities - on which your child is identifiable - through their communication channels (newspaper, magazine, website ...), to illustrate an article about _____ activities? | O | O |
| Can national press publish photos of activities - on which your child is identifiable - through their communication channels (newspaper, magazine, website ...), to illustrate an article about _____ activities? | O | O |
| Can specialized press publish photos of activities - on which your child is identifiable - through their communication channels (newspaper, magazine, website ...), to illustrate an article about _____ activities? | O | O |
| May we use photos / videos of activities - where your child is identifiable – for communication with the project partners about and for reporting (leaflet, project website, educational material) of our activities within the _____ project? | O | O |

The undersigned confirms the choice of these data processes in the context of the stated purposes. If _____ wants to aim at other goals, then the permission for this will be asked separately.

Name parent and name child:

……

……

Date: …… / …… / 20……

Signature parent:

……

## 6.2. Inventory of processing activities

IEECP is data controller and processes only the data which it controls. The other IEECP data is controlled by outside processors, which are all mentioned in the *Data controller inventory* table which is available at this link and will be kept up to date. The table with current inventory is available below.



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

To have a common approach toward providing accountability and compliance with the provisions of the EU GDPR, and to enable IEECP to have a clear view of its processing activities, the Inventory of Processing Activities can be used to record and keep track of IEECP's processing activities of personal data.

It is an internal document which can help IEECP employees to better understand how, and why, personal data needs to be processed and it ensures that IEECP is aware and in control of its data operations.

Since IEECP does not have departments nor is the division of tasks always the same, but rather depends on project activities**, each project leader** is responsible for updating this Inventory whenever he/she is responsible for data controlling or processing. The managing director **Vlasios Oikonomou** can, as an overall person responsible for GDPR, delegate certain inventory handling to another person or can instruct an inventory to be deleted.

Currently, for the implementation of the organisation's activities, IEECP is not processing any data that carry a risk nor processes sensitive data, as showed on the Data Controller Inventory (below). However, IEECP might act as data controller in projects that process special categories of data. In which case, information will be detailed in the Data Controller Inventory excel, which will be kept up to date.



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

## Data controller inventory

| **Responsible person/processor**<br>A processor can be:<br>-an outside agency<br>-a cloud provider that stores personal data<br>-any service provider acting on our behalf with access to personal data of a customer/ employee | **Entry date** | **Purpose of processing activities** | **The recipients to whom the personal data have been or will be disclosed, incl. recipients in 3rd countries** | **Categories of personal data being processed** | **Proposed time limits for erasure of each data category (See description under the table ****)** | **Other information (See descriptions under the table *, **, ***)** |
|---|---|---|---|---|---|---|
| Microsoft | 01.03.21 | Administration of employees' personal data | Managing Director | Personal employee data: name, surname, date of birth, bank accounts, address and telephone number, and medical records/confirmations when they are on sick leave | 7 years after employment for the 'basics' like Name, date of employment, salary information (tax), employment conditions<br><br>2 years for the 'majority' of information: the contract, correspondence about appointments, promotion / demotion and dismissal, reports of performance interviews and appraisal interviews, correspondence with the company doctor, Problem Situation Reports (including Financial Problems)<br><br>1 year for information like CV, references and letters of recommendation. For non-hired applicants this is a maximum of 4 weeks unless the person is informed that you'd like to extend this | / |
| EKSTRATEGIES | 01.03.21 | Payroll information | Managing Director | Personal employee data: name, surname, date of birth, bank accounts, address and telephone number, and medical records/confirmations when they are on sick leave | 5 years for tax statements (payroll) and a copy of identification (passport) | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Microsoft | 01.03.21 | Application management/Recruiting | Employee supporting with recruitment | Personal applicant data: name, surname, date of birth, address and telephone number | For rejected applicants maximum 4 weeks after the rejection. | |
| Microsoft | 01.03.21 | Email service for employees and intranet (Microsoft Office 365) | Vlasios Oikonomou<br>Mia Dragović Matosović<br>Filippos Anagnostopoulos<br>Ivana Rogulj<br>Marine Perrio<br>George Stravodimos<br>Chris Kostilas | Personal employee data: name, surname, date of birth | 1 month after the contract with the employee is terminated | |
| MailPoet, **Google** Analytics, **Twitter, Facebook and LinkedIN own analytics tools** | 01.03.21 | Website operation and tracking, newsletter subscription management and social media accounts | Managing Director<br><br>Marine Perrio as Communications Manager | Personal data are kept only for newsletter subscription: name, surname, organization, e-mail address (with only email address as compulsory).<br><br>Website analytics tool (Google Analytics) collects IP location, and events (openings, clicks) but no personal data is available to the communications manager / IEECP. All data is anonymized. | When subscribers unsubscribe or by hand of the communications manager, periodic deletion of the unconfirmed, bounced or unsubscribed accounts | |
| Microsoft | 01.03.21 | Achieve project's objectives - Obligation under Grant Agreement of each project to share responsibilities and | Project team | Personal data of project partners' team: name, surname, company address and telephone, e-mail account, and, if they are a project partner of projects which we | 5 years after the termination of the project | |



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

| | | | | | | |
|---|---|---|---|---|---|---|
| | | work on the projects with other project beneficiaries | Potentially EC unit responsible for the project | coordinate, the company bank account. | | |

*In case there is transfer of personal data to a third country, name the third country and describe suitable safeguards for exceptional transferring personal data (please consult the Advisera Standard Contractual Clauses in folder 8 of the official GDPR Toolkit).

**If the company is processing the personal data together with other companies, then specify the name of this other company ("Joint controller").

*** Where possible, include a general description of the technical and organizational security measures.

**** https://www.dpp-gdpr.com/news/retention-of-employee-data/#:~:text=%E2%80%9CShould%20personal%20data%20be%20deleted,tax%20year%20according%20to%20HMRC



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

## 6.3. Data retention policy and schedule

Whenever personal data is collected, the required retention period set forth in the below table should be respected and the minimum standards set in this section should be applied when destroying certain information within.

This Data Retention Policy applies to all IEECP officers, directors, employees, agents, affiliates, contractors, consultants, advisors or service providers that may collect, process, or have access to data (including personal data and / or sensitive personal data). It is the responsibility of all of the above to familiarise themselves with the rules set within and ensure adequate compliance with it.

This policy applies to all information used at IEECP, such as: emails, hard and soft copy documents, video, audio, etc.

| **Data retention schedule** | | |
|---|---|---|
| **Personal data record category** | **Mandated retention period*** | **Record owner** |
| Payroll records | Seven years after audit | Vlasios Oikonomou and EKSTRATEGIES |
| Supplier contracts | Seven years after contract is terminated | Vlasios Oikonomou and EKSTRATEGIES |
| Emailing system (newsletter subscribers) | Data is deleted either by the subscriber when unsubscribing or by the communications manager when the email address seems out of service. | MailPoet + Communications manager |
| Google Analytics (website statistics) | Data is deleted once the visitor has exited the website | Google Analytics + Communications manager |

*There are three possibilities for defining this retention period:
a) Mandated period is mentioned in the local legislation – e.g. tax, labour, archiving and similar laws;
b) Deletion might be triggered by an event – e.g. the data to a customer might be deleted once the product is delivered; once the visitor has exited the website;
c) The Data Protection Officer defines a reasonable period for data retention.

As an exemption, retention periods within Data Retention Schedule can be prolonged in cases such as:

- Ongoing investigations from Member States authorities, if there is a chance records of personal data are needed by the Company to prove compliance with any legal requirements, such as an audit from an EU authority regarding projects that IEECP was coordinating; or
- When exercising legal rights in cases of lawsuits or similar court proceeding recognized under local law.

### Safeguarding of Data during Retention Period

The possibility that data media used for archiving will wear out shall be considered. If electronic storage media are chosen, any procedures and systems ensuring that the information can be accessed during the retention period (both with respect to the information carrier and the readability of formats) shall also be stored to safeguard the information against loss as a result of future technological changes. Vlasios Oikonomou will appoint one person each year to act a person responsible to check whether

data retention schedules are being adhered to. Usually this is done by the IT manager, so this appointed person should be familiar with IT services used in IEECP.

## Destruction of Data

The Company and its employees should therefore, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant. Overall responsibility for the destruction of data falls to each responsible person on a project, for that project. The person appointed by Vlasios Oikonomou should check with all project leaders and other senior functions whether they have reviewed and deleted their data that they manage.

Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding. The Document Disposal Schedule section below defines the mode of disposal.

In this context, the employee shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that IEECP subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and the Company's Personal Data Protection Policy shall be complied with. Currently, IEECP is performing these activities in-house.

Appropriate controls shall be in place that prevent the permanent loss of essential information of the company as a result of malicious or unintentional destruction of information – these controls are described in folder 8 of Advisera templates.

The Managing Director Vlasios Oikonomou shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

## Breach, Enforcement and Compliance

The person appointed by Vlasios Oikonomou each year for auditing responsibility for Data Protection has the responsibility to ensure that each employee complies with this Policy.

Any suspicion of a breach of this Policy must be reported immediately to Vlasios Oikonomou. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate.

Failure to comply with this Policy may result in adverse consequences, including, but not limited to, loss of beneficiary confidence, litigation and loss of competitive advantage, financial loss and damage to the Company's reputation, personal injury, harm or loss. Non-compliance with this Policy by permanent, temporary or contract employees, or any third parties, who have been granted access to Company premises or information, may therefore result in disciplinary proceedings or termination of



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

their employment or contract. Such non-compliance may also lead to legal action against the parties involved in such activities.

### Document Disposal schedule and destruction method

**Routine Disposal Schedule**

Records which may be routinely destroyed unless subject to an on-going legal or regulatory inquiry are as follows:

- Announcements and notices of day-to-day meetings and other events including acceptances and apologies to the meeting;
- Requests for ordinary information such as travel directions;
- Reservations for internal meetings without charges / external costs;
- Transmission documents such as letters, fax cover sheets, e-mail messages, routing slips, compliments slips and similar items that accompany documents but do not add any value;
- Message slips;
- Superseded address list, distribution lists etc.;
- Duplicate documents such as CC and FYI copies, unaltered drafts, snapshot printouts or extracts from databases and day files;
- Stock in-house publications which are obsolete or superseded; and
- Trade magazines, vendor catalogues, flyers and newsletters from vendors or other external organizations.

In all cases, disposal is subject to any disclosure requirements which may exist in the context of litigation, for example in the case of EU project Audit.

**Destruction Method**

Documents that include any personal data or those that do not include any personal data but contain confidential information such as parties' names, signatures and addresses which could be used by third parties to commit fraud, shall be subject to secure electronic deletion.

## 7. Organisation and responsibilities

The responsibility for ensuring appropriate personal data processing lies with everyone who works for or with IEECP and has access to personal data processed by IEECP.

As mentioned, d**ue to IEECP size we agreed not to have a data protection officer, but instead our managing director Vlasios Oikonomou is in charge of delegating all data protection matters which concern IEECP in general and not the specific projects run by IEECP.** Vlasios Oikonomou is also responsible for making data safety and security decisions for most sensitive matters. Each employee that is also a project coordinator is responsible for ensuring that personal data and data safety and security guidelines mentioned in this document are also followed on that particular project.

Other employees might also act as data controllers or processors for certain projects they manage. Some sections of this document name a position or a person who is responsible for a certain process. **If the person or a position is not explicitly names, this means that the managing director is responsible for delegating this activity and making sure that it is accomplished.**



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

The key areas of responsibilities for processing personal data lie with the following organisational roles:

**The Managing Director** makes decisions about, and approves, IEECP's general strategies on personal data protection. The Managing Director is responsible for ensuring that new employees are familiarised with this policy. He also appoints person(s) responsible for the annual update of this policy and all the accompanying documents. This **appointed employee** is then responsible for checking how the personal data protection program is being implemented and for the development and promotion of end-to-end personal data protection policies.

Section Annex 15.2 gives a short overview of obligation of all IEECP employees.

Any leader of a certain project in which IEECP is a partner or a coordinator is responsible of ensuring that this certain project also follows the fair processing guidelines outlined in this policy.

The **Communications manager** is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.

Although we do not have an **IT manager**, one person will be appointed by the Managing Director each year to:

- Ensure all systems, services and equipment used for storing data meet acceptable security standards.
- Perform checks and scans to ensure security hardware and software is functioning properly.

Any employer undergoing a **procurement process** is responsible for passing on personal data protection responsibilities to suppliers and improving suppliers' awareness levels of personal data protection (for example by referring to this policy) as well as flow down personal data requirements to any third party a supplier they are using. The Procurement Department must ensure that IEECP reserves a right to audit suppliers.

# 8. Guidelines for establishing the lead supervisory authority

Although IEECP employees work across different EU countries, IEECP is registered only in the Netherlands and there is only one lead supervisory authority – IEECP, Netherlands. Thus, the Dutch Data Protection Authority is considered as the lead National supervisory authority.

# 9. Security of personal data

## 9.1. IT Security policy

IT security policy means the rules to use information systems and assets, access policies and security procedures.

By information systems, in case of IEECP, the focus is on the use of software and related data since the other systems are not shared. The information assets in IEECP include equipment like paper documents, portable computers, data storage media, etc. Information assets in the case of IEECP may



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

be used for business needs with the purpose of executing organization-related tasks, but also for the personal needs if used without danger for data breech. It is prohibited to use information assets in a manner that unnecessarily takes up capacity, weakens the performance of the information system or poses a security threat. It is also prohibited to download software or program code, without adequate security check. Relevant anti-virus program must be installed on each computer with activated automatic updates.

Each information asset has a user designated in the Inventory of Assets, managed by Ekstrategies. The asset user is responsible for the confidentiality, integrity and availability of information for the asset in question. Employees must take care of the copyright and never make unauthorized copies of software owned by the organization, except in cases permitted by law. Also, employees must not copy software or other original materials from other sources and are liable for all consequences that could arise under the intellectual property law.

Due to the fact the employees do not share internet infrastructure, IT infrastructure and place of work, additional policies for access, encryption and disaster recovery are not considered needed.

## Backup procedure

All employees must store all the important information stored on their computer to the joint sharing system (*in this case MS SharePoint*) at least once a day. To safeguard the data uploaded, IEECP uses two- factor authentication and logs out inactive users. For data security of the cloud documents, IEECP relies on detailed MS policies. Employees should take care when creating folders shared with guests, and limit those to specific task – related folders.

All documents should be backed up for the period defined in the relevant legal document (contract) or until the termination of the employee's contract.

## User accounts and access

Employees may only access those information system assets for which they have been explicitly authorized by the asset owner (in this case project coordinator or organization management), meaning only the documents that have been shared with them. They may use the information system only for purposes for which they have been authorized, i.e. for which they have been granted access rights and must not take part in activities which may be used to bypass information system security controls. The employee must not, directly or indirectly, allow another person to use his/her access rights, i.e. username, and must not use another person's username and/or password. The owner of the user account is its user, who is responsible for its use, and all transactions performed through this user account. Employees must apply good security practices when selecting and using passwords (not to share them, write down, send trough any channels, use a strong password and change it regularly).

## Data and information exchange methods

When exchanging messages and materials, it could be done via email, Internet transfer via MS SharePoint/MS Teams, different text messaging channels (Skype), mobile phone, portable media and trough different social networks.

Users may only send messages containing true information. It is forbidden to send materials with disturbing, unpleasant, sexually explicit, rude, slanderous or any other unacceptable or illegal content



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

through official IEECP channels. Users must not send spam messages to persons with whom no business relationship has been established or to persons who did not require such information. Should a user receive a spam e-mail, he/she must inform responsible person (in this case project manager, managing the channel, or any of the IEECP MS admins (as mentioned in the data controller inventory table). If confidential, messages should be labelled as such.

The user must save each message containing data significant for the organization's business as described in the documents storing section. Should an employee post a message on a message exchange system (social networks, forums, etc.), he/she must unambiguously state that it does not represent the organization's viewpoint.

## 9.2. Termination of contract

Upon termination of an employment contract or other contract on the basis of which various equipment, software or information in electronic or paper form is used, the user must return all such information assets to Managing Director.

Upon change of contractual relations with external parties who have access to systems, services and facilities, or upon expiration of the contract, contract owner must immediately inform the responsible persons who approved privileges for the external parties in question. The access rights for all the persons who have changed their employment status or contractual relationship must immediately be removed or changed by responsible persons. E-mail address will be archived with automatic response.

## 9.3. Teleworking and using own devices policy

Teleworking means that information and communication equipment is used to enable employees to perform their work outside the organization and the work in IEECP is organized as teleworking for all employees. For teleworking, ensuring the following is crucial:

- protection of computing equipment as specified in the previous section,
- prevention of unauthorized access by persons living or working on the location where the teleworking activity is performed, which is described under clean desk and screen policy below,
- appropriate configuration of the local network used for connecting to the Internet,
- protection of the organization's intellectual property rights, either for software or other materials that may be protected by intellectual property rights,
- process for return of data and equipment in the case of termination of employment, as described in the previous section, via authorized courier.

### Clean desk and clean screen policies in teleworking:

If the employee is not at his/her workplace, all confidential paper documents, as well as data storage media labelled as sensitive (for example containing personal data on salaries etc.), must be removed from the desk or other places (printers, fax machines, photocopiers, etc.) to prevent unauthorized access by visitors, roommates and family members. Such documents and media must be stored in a secure manner. If the employee is not at his/her workplace, all sensitive information must be removed from the screen, and access must be denied to all systems for which the person has authorization, using password screen lock.



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

This section is especially relevant if using co-working spaces or working hubs.

### Bring your own device (BYOD) policy

IEECP supports widespread use of BYOD for work use – i.e. using such devices for performing work for the company for all employees.

The company data that is stored, transferred or processed on BYOD remains under the IEECP ownership, and IEECP retains the right to control such data even though it is not the owner of the device. IEECP has the right to view, edit, and delete all company data that is stored, transferred or processed on BYOD, while protecting the personal data of the owner.

IEECP will not pay the employees (the owners of BYOD) any fee for using the device for work purposes or the telecommunication costs but will pay for any new software that needs to be installed for organizational use.

## 10. Response to Personal Data Breach Incidents

When employee learns of a suspected or actual personal data breach, he or she is obliged to inform the managing director **Vlasios Oikonomou, who must designate an employee who will perform an internal investigation and take appropriate remedial measures in a timely manner**, according to the below described Data Breach Policy. If the subject is considered of any risk for the person whose data has been involved in an incident, a Team of two employees will be appointed. Where there is any risk to the rights and freedoms of data subjects, IEECP must notify the relevant data protection authorities/EU representative without undue delay.

The report to the relevant authorities shall include the following information:

- Content of the data breached, number of affected subjects, list of consequences, measures taken, and contacts involved.

Designated employee or team oversees also informing the data subject(s), with the details on:

- What has happened to the person's data (disclosed, destroyed, lost or similar), what are possible consequences and the measures taken.

## 11. Audit and accountability

Each year the Managing Director, Vlasios Oikonomou will appoint a person in IEECP who will be responsible for auditing how well business P implement this Policy.

Any employee who violates this Policy will be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations.

## 12. Conflicts of law

This Policy is intended to comply with the laws and regulations in the place of establishment (the Netherlands) and of the countries in which it operates its projects. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

## 13. Managing records kept on the basis of this document

| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
|---|---|---|---|---|
| **Data Subject Consent Forms** | link | Each project manager for their project, Marine Perrio for IEECP related publications, such as the newsletter contact list | Only authorized persons may access the forms | 10 years |
| **Data Subject Consent Withdrawal Form** | link | Each project manager for their project, Marine Perrio for IEECP related publications, such as the newsletter contact list | Only authorized persons may access the forms | 10 years |
| **Supplier Data Processing Agreements** | link | Vlasios Oikonomou | Only authorized persons may access the folder | 5 years after the agreement has expired |
| **Register of Privacy Notices** | The locations are available in a table in section 6.1 of this document | Marine Perrio | Only authorized persons may access the folder | Permanently |
| **Processor GDPR Compliance questionnaire** | We do not have such a questionnaire, but when we do, it should be entered in this table! | | | 5 years after the contract has expired |

## 14. Validity and document management

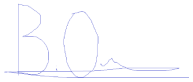
This document is valid as of the signing of the Managing Director. This implies that there was an online team meeting describing the rights and obligations from this document to all IEECP staff.

The owner of this document is the Managing Director Vlasios Oikonomou, who must, at least once a year, designate a person who will check and, if necessary, update the document as needed.

Managing Director
Vlasios Oikonomou

*Electronic signature here*

Signed by:Vlasios Oikonomou
Signed at:2021-05-24 11:17:54 +00:00
Reason:Witnessing Vlasios Oikonomou





Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

# 15. Annexes

## 15.1. Template Data Management Plan for EU projects

### 1. Data Summary

| *As much as possible, answer the following questions:* |
|---|
| What is the purpose of the data collection/generation and its relation to the objectives of the project? |
| What types and formats of data will the project generate/collect? |
| Will you re-use any existing data and how? |
| What is the origin of the data? |
| What is the expected size of the data? |
| To whom might it be useful ('data utility')? |

### 2. FAIR data

#### 2. 1. Making data findable, including provisions for metadata

| *As much as possible, answer the following questions:* |
|---|
| Are the data produced and/or used in the project discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)? |
| What naming conventions do you follow? |
| Will search keywords be provided that optimize possibilities for re-use? |
| Do you provide clear version numbers? |
| What metadata will be created? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how. |

#### 2.2. Making data openly accessible

| *As much as possible, answer the following questions:* |
|---|



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

Which data produced and/or used in the project will be made openly available as the default? If certain datasets cannot be shared (or need to be shared under restrictions), explain why, clearly separating legal and contractual reasons from voluntary restrictions.

Note that in multi-beneficiary projects it is also possible for specific beneficiaries to keep their data closed if relevant provisions are made in the consortium agreement and are in line with the reasons for opting out.

How will the data be made accessible (e.g. by deposition in a repository)?

What methods or software tools are needed to access the data?

Is documentation about the software needed to access the data included?

Is it possible to include the relevant software (e.g. in open source code)?

Where will the data and associated metadata, documentation and code be deposited? Preference should be given to certified repositories which support open access where possible.

Have you explored appropriate arrangements with the identified repository?

If there are restrictions on use, how will access be provided?

Is there a need for a data access committee?

Are there well described conditions for access (i.e. a machine readable license)?

How will the identity of the person accessing the data be ascertained?

## 2.3. Making data interoperable

***As much as possible, answer the following questions:***

Are the data produced in the project interoperable, that is allowing data exchange and re-use between researchers, institutions, organisations, countries, etc. (i.e. adhering to standards for formats, as much as possible compliant with available (open) software applications, and in particular facilitating re-combinations with different datasets from different origins)?

What data and metadata vocabularies, standards or methodologies will you follow to make your data interoperable?

Will you be using standard vocabularies for all data types present in your data set, to allow inter-disciplinary interoperability?

In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies?



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

### 2.4. Increase data re-use (through clarifying licences)

***As much as possible, answer the following questions:***

How will the data be licensed to permit the widest re-use possible?

When will the data be made available for re-use? If an embargo is sought to give time to publish or seek patents, specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.

Are the data produced and/or used in the project useable by third parties, in particular after the end of the project?

If the re-use of some data is restricted, explain why. How long is it intended that the data remains re-usable? Are data quality assurance processes described?

## 3. Allocation of resources

***As much as possible, answer the following questions:***

What are the costs for making data FAIR in your project?

How will these be covered? Note that costs related to open access to research data are eligible as part of the Horizon 2020 grant (if compliant with the Grant Agreement conditions).

Who will be responsible for data management in your project?

Are the resources for long term preservation discussed (costs and potential value, who decides and how what data will be kept and for how long)?

## 4. Data security

***As much as possible, answer the following questions:***

What provisions are in place for data security (including data recovery as well as secure storage and transfer of sensitive data)?

Is the data safely stored in certified repositories for long term preservation and curation?

## 5. Ethical aspects



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

*NOTE: This chapter may be removed in case this information is already explained in another report (e.g., Ethics Report). In which case, the DMP can refer to the report.*

***As much as possible, answer the following questions:***

Are there any ethical or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).

Is informed consent for data sharing and long term preservation included in questionnaires dealing with personal data?

## 6. Other issues

*NOTE: This chapter may be removed in case this information is already explained in other report(s) (e.g., Ethics Report). In which case, the DMP can refer to the report.*

***As much as possible, answer the following questions:***

Do you make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones?

## 15.2 Yearly GDPR audit checklist

This checklist is meant to help all IEECP employees to adhere to tasks and policies set out in this plan.

It does not replace reading through the entire plan, but please use it to check whether you have ensured that all procedures described here are followed!

| Person in charge | Activity | Related section in Data Protection Policy |
|---|---|---|
| **Managing director**: | | |
| | Each year appoints one "**Data Protection Manager**" – a person responsible for checking the adherence to Data Protection Policy and updating it. This person is also responsible to ensure that there is a team meeting where all employees are familiarised with the changes in the Policy. | |
| | Each year appoints one "**IT person**" to check Data retention and deletion. This person should:<br>-Check with all project leaders and other senior functions whether they have reviewed and deleted their data that they manage.<br>-Ensure all systems, services and equipment used for storing data meet acceptable security standards.<br>-Perform checks and scans to ensure security hardware and software is functioning properly. | section 6.3 |



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

| | | |
|---|---|---|
| | Approves the destruction process of any documents that the appointed "IT person" in charge of checking Data Retention and deletion advises should be destroyed. | |
| | Authorises the changes made in the document and sign the Policy newest version | |
| | When any contract is being signed, please check that all activities under category "Any employee contracting a 3rd party to do business with or for IEECP" are performed | |
| | If there is a data breach, designate an employee who will perform an internal investigation and take appropriate remedial measures in a timely manner | section 10 |
| **Project manager (the main person responsible for a certain project)**: | | |
| | Ensure that the project has its own Data Management Plan - check annex 15.1 for a proposed template of an EU project Data Management Plan. If you are the coordinator, check who in your project is the data controller and ensure that the listed activities are taken care of. | annex 15.1 |
| | If data is being collected by IEECP in this project, then please check the category "any employee collecting personal data" | |
| **Any employee collecting personal data:** | | |
| | Ensure right of access by data subjects | Section 5.7 |
| | Ensure data portability | Section 5.8 |
| | Right to be forgotten | Section 5.9 |
| | If a subject whose information is being collected by IEECP requests any change or deletion, the request must be saved in the designated folder "Log of requests" | |
| | Perform DPIA when starting the project to decide whether any additional data protection actions are necessary | section 6 |
| | At any point when you collect personal data, inform the subjects of our Privacy and cookie Notice (updated version is always available on IEECP's website). | |
| | Where **sensitive** personal data is being collected, ensure that the Privacy Notice explicitly states the purpose for which this sensitive personal data is being collected. | |
| | In case there is a new Privacy policy, make sure to include it in the Plan, table "Registry of Privacy Notices" | Section 6 |
| | Update the Data Controller Inventory table to show which data is being collected | Link |
| **Communications Manager**: | | |
| | Make sure that the Privacy and cookie policy (GDPR articles 12 and 13), the newsletter privacy notice and data subject consent forms are updated | Section 6 |
| | All actions same as "An employee collecting personal data", but for general IEECP communication channels which are not project specific | |
| | Approving any data protection statements attached to communications such as emails and letters. | |
| | Addressing any data protection queries from journalists or media outlets like newspapers. | |
| **Any employee contracting a 3rd party to do business with or for IEECP**: | | |
| | Conduct a Processor GDPR Compliance questionnaire | Section 5.5 |
| | Perform DPIA when starting a new process/activity or a relationship with 3rd party to decide whether any additional data protection actions are necessary | section 6 |
| | If personal data is being collected, please check category "Any employee collecting personal data" | |



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org

| **All employees**: |
| --- |
| Read the Data Protection Policy each year |
| Check whether you are collecting any personal and perhaps sensitive data |
| Be aware of how long you keep documents and emails with personal data |
| If you suspect of any irregularities or data breaches, report to Vlasis immediately |



Institute for European Energy and Climate Policy Stichting, Amsterdam Sloterdijk Teleport Towers, Kingsfordweg 151, 1043GR Amsterdam, The Netherlands; KvK: 64602214; VAT: NL0855739198B01; www.ieecp.org ; info@ieecp.org