HEATERNAL

Deliverable D1.3

GDPR compliance report

Date : 26/10/2023
Deadline : 30/09/2023

Claire HOUZÉ

Funded by the European Union

Document Control Sheet

PROJECT INFORMATION

Project Number	101103921		
Project Acronym	HEATERNAL		
Project Full title	innovative High tEmperAture ThErmal stoRage for iNdustrial AppLications		
Project Start Date	01/05/2023		
Project Duration	42 months		
Funding Instrument	Horizon Europe	Funding Scheme	
Topic	Development of high temperature thermal storage for industrial applications		
Coordinator	CEA		

DELIVERABLE INFORMATION

Deliverable No	**1.3**
Deliverable Title	**GDPR compliance report**
Work-Package No	1
Work-Package Title	Project Manager
WP-Leader (Name and Short Org. Name)	Sylvie DOUARD (CEA)
Task No	1.2
Task Title	Operationnal Management
Task Leader (Name and Short Org. Name)	Claire HOUZÉ (CEA)
Main Author (Name and Short Org. Name)	Claire HOUZÉ (CEA)
Other Authors (Name and Short Org. Name)	Sylvie DOUARD (CEA) ; Ana FERNANDER (SPI)
Reviewers (Name and Short Org. Name)	Sylvie DOUARD (CEA), Claire HOUZÉ (CEA)
Status	Draft ☐ Final ☒
Deliverable Type	Report ☒ Data ☐ Demonstration ☐ Other ☐
Dissemination Level	Public (PU) ☒ Sensitive (SEN) ☐ Classified ☐ PU: Public, fully open SEN: Sensitive, limited under the conditions of the Grant Agreement Classified R-UE/EU-R – EU RESTRICTED under the Commission Decision No2015/444 Classified C-UE/EU-C – EU CONFIDENTIAL under the Commission Decision No2015/444 Classified S-UE/EU-S – EU SECRET under the Commission Decision No2015/444
Date Approved by Coordinator	26/10/2023

DOCUMENT VERSION HISTORY

Version	Date	Author	Description of Change
V1.0	13/10/2023	Claire HOUZÉ (CEA)	First version
V2.0	24/10/2023	Ana Fernandes (SPI)	Processes verifications

DOCUMENT REVIEW

Reviewer	Date	Reviewer Name (Short Organisation Name)
Work Package learder	26.10.2023	Sylvie Douard (CEA)
Project Manager	24.10.2023	Claire Houzé (CEA)
Exploitation Manager	24.10.2023	Ana Fernandes (SPI)
Coordinator	26.10.2023	Sylvie Douard (CEA)

Legal disclaimer

This project has received funding from the European Union's Horizon Europe research and innovation program under grant agreement No. 101103921

Table of contents

Index of tables

Executive Summary

Heaternal project will be compliant with national and EU legislation within the area of personal data. This deliverable provides an explanation on how the project will handle personal data.

1. Introduction

The HEATERNAL consortium is committed to ensuring GDPR compliance. Two aspects of the project will require collecting and managing personal data.

- Firstly, SPI will collect personal data for dissemination, communication and networking beyond the consortium.
- Secondly, CEA, as Project Coordinator & Project Manager, will be responsible for maintaining the partner contact database for overall project management.

This next section summarises the type of data that will be collected in both cases. The relevant GDPR policies are provided in the annexes of this deliverable.

2. Types of data collected by HEATERNAL

Why it is collected and an overview of the GDPR policy.

2.1 SPI – Personal Data for Communication, Dissemination and Networking

In order to build the contact database for HEATERNAL (for WP8), SPI will collect personal contact data. The SPI confirms that all of the data intended to be processed are relevant and limited to the purposes of the research project (in accordance with the 'data minimization principle' of the GDPR regulation). The purpose is to ensure the dissemination, replication and broad uptake of the results of the HEATERNAL project. The personal data will be limited to:

- Name (mandatory)
- Organisation (mandatory)
- Title (mandatory)
- Email address (mandatory)
- Telephone number (optional)

SPI confirms that it has appointed a Data Protection Officer (DPO), Douglas THOMPSON of SPI. The DPO can be reached to the following email address : info@heaternal.eu, it will be provided on the HEATERNAL website and in all newsletters and invitations to events so that all data subjects involved in HEATERNAL can request that their data be erased.

For further processing of previously collected personal data, SPI has lawful basis for the data processing and the appropriate technical and organizational measures are in place to safeguard the rights of the data subjects. Detailed information on the informed consent procedures in regard to data processing are kept on file by SPI.

A description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects can be found below and in SPI's GDPR policy in Annex 1 below.

Regarding informed consent, the following cases apply.

A data subject can sign-up to be added to the HEATERNAL contact list via the HEATERNAL website.

When SPI shall receive the contact information from an interested entity, the link to the informed consent form will be sent by email to the data subject. If no consent is received from the contact, then the contact details will not be saved or used by SPI. Indeed any information about HEATERNAL project will be sent to the subject's contact.

HEATERNAL's Informed consent form will include the following information:

If you would like to join the HEATERNAL Community, please provide your:

- Last name,
- First name,
- Professional telephone numbers
- Professional email address,
- Employer entity,
- Job title.

Please specify for which purpose you consent to be contacted:

- To receive the HEATERNAL 3-monthly newsletters,
- To be invited to HEATERNAL annual workshops,
- To be contacted by a HEATERNAL partner in order to discuss project results and possible collaborations individually.

Anyone who has communicated personal data to SPI has the following rights over it:

- The right of access, modification or rectification,
- The right to erase the data (right to be forgotten), a right to limit processing and a right to object to processing in the cases provided for by the regulations in force,
- The right to define directives relating to the fate of his personal data after his death,
- The right to the portability of the raw data transmitted to the cluster,
- The right to file a complaint with the competent authority (for example, the CNIL in France),
- The right to object to the receipt of newsletters, emails or invitations.

These rights must be exercised under the conditions provided for by the regulations in force. In particular, proof of identity may be requested. These rights can be exercised by preferably sending an e-mail request to info@heaternal.eu or via post to the following address:

SPI
Avenida Marechal Gomes da Costa, 1376
4150 - 356 Porto

Unless you request that your data be erased, then collected data will be stored for the minimum period of time necessary for the purposes described in the consent form or at least for the duration of the project plus one year. After this period, collected data will be removed from the database.

Regarding the storage, correction, use and erasing of personal data in the scope of HEATERNAL:

- Personal data handled by SPI within the scope of HEATERNAL will be collected, stored and processed only within SPI's partner relationship management tool, Excel files located on SPI's

internal servers only accessible with an SPI computer, which is a GDPR-compliant and secure tool. Password protected access is limited to SPI staff, the service provider, SPI's website developer and the HEATERNAL website developer.

- If a data subject requests that their data be corrected, SPI will correct the data in the CRM.
- If a data subject requests that their data be erased, SPI's DPO will erase the data subject in the Excel files.
- The voluntary forms on HEATERNAL's website will feed personal contact data and the purpose for which SPI has the right to use the contact data to SPI's Excel files.
- The Newsletters and invitations to HEATERNAL events will be sent only to those contacts having given consent for each type of emailing, through Sendblaster platform compliant with GDPR rule.
- Each emailing will offer the possibility to cancel the subscription to that type of emailing or to request corrections / erasure by sending an email to info@heaternal.eu

2.2 CEA – Personnal Data for overall project management

CEA, as project coordinator, will have to maintain and up-date the partners contact list for daily operational management and strategic decision making (WP1). CEA has created an online, shared project space for collaborative work and has set up a secure repository for maintaining the partner contact database for overall project management. To this end, CEA will collect email address, phone numbers, names, positions and names of employers for both the shared online space and contact lists for partners.. The Data Policies of CEA are found in Annex 2.

2.3 LOMARTOV – Personal Data collecting for Techno-economic analysis, Environmental Life Cycle Assessment, Social Life Cycle Assessment and stakeholder analysis

LOMARTOV, as Heaternal work package leader (WP7) will have to collect personal data of the consortium members and skateholders to undertake the tasks planned in their WP.

1. For undertaking the Techno-economic analysis, TEA (Task 7.1), the Environmental Life Cycle Assessment, LCA (Task 7.2) and the Social Life Cycle Assessment, s-LCA (Task 7.3.), LOMARTOV will use professional databases such as Social hotspot database and Eco-invent, for which they already have an authorisation. In addition, LOMARTOV will collect data from the members of the consortium to perform these analyses. In this case, data protection and confidentiality are covered by the Grant Agreement and the Consortium Agreement. If a member of the consortium wishes to have a Non Disclosure Agreement (NDA)/Consent form, LOMARTOV is ready to sign it, and if these analyses involve collecting data from an entity or a department outside of the consortium, they are also ready to sign a Non Disclosure Agreement (NDA)/consent form.

2. The stakeholder analysis (Task 7.3: Social sustainability: Responsible R&I, acceptance & awareness) will involve collecting the following data including contact details: name, position, email address, name of company/organisation they work for and type, relevance to HEATERNAL framework. This data will remain within the consortium, will be GDPR compliant and will not be disseminated publicly without the formal consent of the participants.

Where needed and to complement the social LCA and the stakeholder analysis above, a quick survey may be undertaken. The results of this survey will be anonymised and will not disclose any type of confidential data or personal data of the participants.

Any personal data that will be collected and processed for undertaking all the activities described above will remain within the consortium and will not be disseminated publicly without the formal consent of the participants.

And any activity undertaken in the framework of the tasks described above will be GDPR compliant.

The deliverables that will be generated by the tasks described above, particularly those with a public dissemination level, will not disclose personal data.

LOMARTOV privacy policy is available in Annex 3.

2.4 Other beneficiary partners

All Heaternal partners will be compliant with the General Data Protection Regulation (GDPR) during their collection of personal data limited to the purposes of the research project in accordance with the ‘data minimisation principle’. Indeed, the partners entities have implemented the organizational measures to safeguard the rights and freedom of the data subjects. Each partner has named a ‘Data Protection Officer’ (DPO) and has set up a privacy policy for their organization.The following table gives the name of the Heaternal partners ‘Data Protection Officer’ and each partner’s privacy policy will be found in Annex 4.

Table 1. List of Partners’ DPOs

Participant N°	Partner entity	DPO name

1	CEA	Laure FLAMAND DE LESTAPIS
2	CICe	Asier URZELAI
3	UGent	Hanne ELSEN
4	LEITAT	Joan Parra PODERES
5	TORRECID SA	Alejandro ROS IGUAL
6	LOMARTOV SL	Lorena ROMERO SANTACREU
7	CALDERYS	Jeannie MONGOUACHON
8	SPI	Douglas THOMPSON
9	ALCOA	ALCOA's Privacy Program Office
10	UGITECH	Thomas BALZER
11	DELAUNEY	Bruno BERNARD

3. Conclusion

This document present the overall GDPR policies that will be applied during all duration of the HEATERNAL Project. Further details can be found in Annexes.

4. Completion level

This deliverable is 100% completed.

5. Annexes

5.1 ANNEX 1 : CEA's GDPR Policy

The CEA, coordinator of HEATERNAL, is a key player in bringing research to industry, especially in low carbon energies. It has extensive experience in thermal storage for various applications and temperature ranges. CEA owns a platform used to design, test and validate innovative energy storage concepts.

To this end, CEA collects and processes certain personal data concerning its members, partners and other contacts for professional purposes. CEA attaches the utmost importance to respecting and protecting the privacy and personal data of its contacts as well as to respecting the regulations in force. The data processing by CEA is carried out according to the methods described below.

5.1.1 Aim and Nature of the collected data

5.1.1.1 CEA's members

The CEA collects personal data concerning its members via the membership form, the member's area of CEA's website, registration for events and subscription to newsletters. This information is collected as part of the management of the organism and the fulfillment of its missions, namely: coordination and management.

The data collected are:

- Last name,
- First name,
- Professional telephone numbers
- Professional email address,
- Employer entity,
- Job title.
- These personal data are used to **:**
- Manage the organism and its general functionning (memberships, etc.),
- Manage event registrations,
- Manage subscriptions to newsletters,
- Carry out satisfaction surveys and polls,
- Manage the contacts file in the CRM,
- Connect members with potential partners,
- Send confidential access codes to the CEA site extranet.

This data processing is based on the execution of a membership contract, the respect by the pole of its legal obligations as well as its legitimate interests for the purposes of the exercise of its activity and the

achievement of its objectives as a competitiveness cluster. In case of refusal to provide the necessary information, the structure will not be able to join the cluster.

5.1.1.2 Non members

The CEA may collect personal data concerning its contacts, suppliers, partners and institutions, in particular the following data:

- Last name,
- First name,
- Professional telephone numbers
- Professional email address,
- Employer entity,
- Job title.

This information can be collected in the different cases listed below:

- Voluntary registration for the organism newsletter or for other newsletters prepared by the organism.
- Complete entry of contact details in a form on CEA's website or any other website administered by CEA (contact, registration, etc.),
- Exchanges between the organism and the person concerned by telephone or e-mail,
- Sending a request for consents by e-mail.

The purposes of the processing of the personal data are as follows:

- To restore the information requested by the data subject if necessary,
- To manage the file of contacts, prospects and partners in the Partner Relationship Management Tool,
- To send invitations to events, webinars, activities and events,
- To send communications and information concerning the cluster's activities.
- The processing is based on the execution of a contract for services provided to companies and the organization of events, demonstrations, the respect by the pole of its legal obligations as well as its legitimate interests for the purposes of the exercise of its activity and achieving its goals. In case of refusal to provide the necessary information, the structure will not be able to benefit from the organized activities and information sent by the pole.

5.1.2 Use of data by CEA

Personal data is subject to processing by the organism for the purposes explained above. The CEA undertakes not to use personal data for any other purpose, or to transmit it to third parties, except in the cases provided for in this data management policy. The CEA may be required to communicate personal

data processed to third parties, at the request of a judicial, administrative or public authority, in the context of compliance with a legal obligation or further to a judicial or administrative decision. Personal data may be communicated by the cluster to its administrators, staff, suppliers and partners. The CEA division takes all necessary measures to require these recipients and subcontractors to comply with applicable regulations.

Personal data is kept for the purposes explained above for the time necessary to achieve these purposes.

- Personal data collected for the execution of a contract or legal obligations are archived for the duration envisaged by the said legal obligation and for the duration necessary for the observation, the exercise or the defense of a legal claim, equivalent to the limitation period applicable to the obligations between the division and the person concerned.
- The personal data used for the purposes of managing the contact file are kept for a period of three years from the last contact between the pole and the person concerned.

The CEA makes every effort to store and archive this personal data under appropriate security conditions in compliance with the applicable provisions, according to current technical means.

5.1.2.1 What rights do subjects have to the personal data communicated?

Anyone who has communicated personal data to CEA has the following rights over it:

- The right of access, modification or rectification,
- The right to erase the data (right to be forgotten), a right to limit processing and a right to object to processing in the cases provided for by the regulations in force,
- The right to define directives relating to the fate of his personal data after his death,
- The right to the portability of the raw data transmitted to the cluster,
- The right to file a complaint with the competent authority (for example, the CNIL in France),
- The right to object to the receipt of newsletters, emails or invitations.

These rights must be exercised under the conditions provided for by the regulations in force. In particular, proof of identity may be requested. These rights can be exercised by sending e-mail request to CEA's DPO at dpd@cea.fr or via post to the following address:

CEA
Bâtiment le Ponant
25 rue Leblanc
75015 Paris

5.1.2.2 Hypertext Links and cookies

Le website www.cea.fr, as well as any website prepared by CEA, contains a number of hypertext links to other sites. However, CEA does not have the possibility to check the content of the sites thus visited, and

therefore will not assume any responsibility. The user should inquire about the privacy and practices of these sites before sending any personal information to them.

The www.cea.fr website, as well as any website that CEA prepares, uses cookies, but it may also use third-party technologies to present a better display and certain services, in particular to track audiences. The user is informed that, during his visits to the website, a cookie can be automatically installed on his browser software. The cookie is a block of data which does not identify the user but is used to record information relating to the browsing of the latter on the website. These are mainly used to study and optimize the user experience on the website.

When visiting, the www.cea.fr website, as well as any website that CEA prepares, the user will be informed upon connection to the website that the website uses cookies. Before gaining access to the page, the user will be given the choice between accepting cookies and learning more. If the user requests to learn more, he or she will gain access to a summary of the GDPR policy of CEA and will be given the choice between:

- Essential and strictly necessary cookies – These are cookies essential for the proper functioning of the site and strictly necessary for the provision of a service that the user has expressly requested. These essential cookies make it possible to memorize from one page to another the information that a user communicates to the website during his/her navigation, for example the language of use.
- Site audience analysis cookies – They allow CEA to establish anonymous statistics of visits to the pages of its site in order to improve its ergonomics and content.

5.2 Annex 2 SPI's GDPR Policies

The leader of dissemination and outreach, SPI, has a public-private network of 370 members (Europe and worldwide) able to reach relevant stakeholders including key partnerships to link innovation projects to early adopter companies.

SPI will collect and process certain personal data concerning its members, partners and other contacts for professional purposes. SPI attaches the utmost importance to respecting and protecting the privacy and personal data of its contacts as well as to respecting the regulations in force. The data processing by CEA is carried out according to the methods described below.

5.2.1 Aim and Nature of the collected data

5.2.1.1 SPI's members

The SPI collects personal data concerning its members via the membership form, the member's area of SPI's website, registration for events and subscription to newsletters. This information is collected as part of the management of the HEATERNAL project and the fulfillment of its missions, namely: communication, dissemination and exploitation.

- The data collected are:
- Last name,
- First name,
- Professional telephone numbers
- Professional email address,
- Employer entity,
- Job title.

These personal data are used to **:**

- Manage the HEATERNAL project and its general functionning (memberships, etc.),
- Manage event registrations,
- Manage subscriptions to newsletters,
- Carry out satisfaction surveys and polls,
- Manage the contacts file in the CRM,
- Connect members with potential partners,
- Send confidential access codes to the SPI site extranet.
- This data processing is based on the execution of a membership contract, the respect by the pole of its legal obligations as well as its legitimate interests for the purposes of the exercise of its activity and the achievement of its objectives as a competitiveness cluster. In case of refusal to provide the necessary information, the structure will not be able to join the cluster.

5.2.1.2 Non members

The SPI may collect personal data concerning its contacts, suppliers, partners and institutions, in particular the following data:

- Last name,
- First name,
- Professional telephone numbers
- Professional email address,
- Employer entity,
- Job title.

This information can be collected in the different cases listed below:

- Voluntary registration for the HEATERNAL project newsletter or for other newsletters prepared by the HEATERNAL project.
- Complete entry of contact details in a form on SPI's website or any other website administered by SPI (contact, registration, etc.),
- Exchanges between the [organism/company/other] and the person concerned by telephone or e-mail,
- Sending a request for consents by e-mail.

The purposes of the processing of the personal data are as follows:

- To restore the information requested by the data subject if necessary,
- To manage the file of contacts, prospects and partners in the Partner Relationship Management Tool,
- To send invitations to events, webinars, activities and events,
- To send communications and information concerning the cluster's activities.
- The processing is based on the execution of a contract for services provided to companies and the organization of events, demonstrations, the respect by the pole of its legal obligations as well as its legitimate interests for the purposes of the exercise of its activity and achieving its goals. In case of refusal to provide the necessary information, the structure will not be able to benefit from the organized activities and information sent by the pole.

5.2.2 Use of data by SPI

Personal data is subject to processing by the [organism/company/other] for the purposes explained above. The SPI undertakes not to use personal data for any other purpose, or to transmit it to third parties, except in the cases provided for in this data management policy. The SPI may be required to communicate personal data processed to third parties, at the request of a judicial, administrative or public authority, in

the context of compliance with a legal obligation or further to a judicial or administrative decision. Personal data may be communicated by the cluster to its administrators, staff, suppliers and partners. The SPI division takes all necessary measures to require these recipients and subcontractors to comply with applicable regulations.

Personal data is kept for the purposes explained above for the time necessary to achieve these purposes.

- Personal data collected for the execution of a contract or legal obligations are archived for the duration envisaged by the said legal obligation and for the duration necessary for the observation, the exercise or the defense of a legal claim, equivalent to the limitation period applicable to the obligations between the division and the person concerned.
- The personal data used for the purposes of managing the contact file are kept for a period of three years from the last contact between the pole and the person concerned.

The SPI makes every effort to store and archive this personal data under appropriate security conditions in compliance with the applicable provisions, according to current technical means.

5.2.2.1 What rights do subjects have to the personal data communicated?

Anyone who has communicated personal data to SPI has the following rights over it:

- The right of access, modification or rectification,
- The right to erase the data (right to be forgotten), a right to limit processing and a right to object to processing in the cases provided for by the regulations in force,
- The right to define directives relating to the fate of his personal data after his death,
- The right to the portability of the raw data transmitted to the cluster,
- The right to file a complaint with the competent authority (for example, the CNIL in France),
- The right to object to the receipt of newsletters, emails or invitations.

These rights must be exercised under the conditions provided for by the regulations in force. In particular, proof of identity may be requested. These rights can be exercised by sending e-mail request to SPI's DPO at douglasthompson@spi.pt or via post to the following address:

SPI
Avenida Marechal Gomes da Costa, 1376
4150 - 356 Porto

5.2.2.2 Hypertext Links and cookies

Le website https://www.spi.pt, as well as any website prepared by SPI, contains a number of hypertext links to other sites. However, SPI does not have the possibility to check the content of the sites thus visited, and therefore will not assume any responsibility. The user should inquire about the privacy and practices of these sites before sending any personal information to them.

The https://www.spi.pt website, as well as any website that SPI prepares, uses cookies, but it may also use third-party technologies to present a better display and certain services, in particular to track audiences. The user is informed that, during his visits to the website, a cookie can be automatically installed on his browser software. The cookie is a block of data which does not identify the user but is used to record information relating to the browsing of the latter on the website. These are mainly used to study and optimize the user experience on the website.

When visiting, the https://www.spi.pt website, as well as any website that SPI prepares, the user will be informed upon connection to the website that the website uses cookies. Before gaining access to the page, the user will be given the choice between accepting cookies and learning more. If the user requests to learn more, he or she will gain access to a summary of the GDPR policy of SPI and will be given the choice between:

Essential and strictly necessary cookies – These are cookies essential for the proper functioning of the site and strictly necessary for the provision of a service that the user has expressly requested. These essential cookies make it possible to memorize from one page to another the information that a user communicates to the website during his/her navigation, for example the language of use.

Site audience analysis cookies – They allow SPI to establish anonymous statistics of visits to the pages of its site in order to improve its ergonomics and content.

5.3 Annex 3 CICe's GDPR Policies

- Data controller

FUNDACIÓN CENTRO DE INVESTIGACIÓN COOPERATIVA DE ENERGÍAS ALTERNATIVAS "CIC energiGUNE" (from now on CIC energiGUNE). Mailing Address: Parque Tecnológico de Álava, Albert Einstein 48 - ED. CIC 01510 MIÑANO (Álava). Email address: info@cicenergigune.com Tfn. 945 29 71 08.

- How we obtained your data

Obtained from the individual concerned: if you are already a client/supplier (current or potential), or a researcher or, for example, if you send us a CV to work with us, you have provided them to us, either off-line or on-line when requesting our services to maintain contact and communication with you, to provide the requested services, to manage your CV or, where appropriate, to keep the contractual relationship with you.

When you provide us your personal data, you guarantee that you are able to provide this information and that it is true, truthful, accurate and up-to-date, that it is not confidential, that it does not violate any contractual restrictions or third party rights and that you undertake not to impersonate other users.

Obtained automatically when visiting our website: If you have provided us with data through this website, we collect information, for example, when you access the page, when you fill out any form with personal data, or when you communicate with us directly by email.

When you visit our website, data is sent from your browser to our server to optimize our services and improve your user experience, for example, when you access the site or when you log in to our services through third party services such as social networks. Such data may be automatically collected and stored by third parties or by us on our behalf. This data may include:

- the user´s IP address
- the date and time of the visit
- the URL of the site the user came from
- the pages visited on our website
- information about the browser used (type and version of the browser, operating system, etc.).

We may process and record such uses, sessions, and related information, either independently or with the help of third-party services, including through the use of "cookies" and other tracking technologies such as flash cookies and web analytics.

If our website has social network connectors, when you choose to interact with us through a social network, we cannot be responsible for the privacy settings selected by the user. The social network may report your IP address or what page you are visiting on our website and may set a cookie to allow it to work correctly, or for example, your name will appear in the likes you give or in the comments you make on our social network page. If you do not want your personal data associated with these "likes" or comments to appear, set your privacy to avoid it, for example, by pseudonymizing your data with a nickname or alias that does not reveal your name and surname.

If you log in to one of these social networks during your visit to our website, the social network will be able to add that information to your profile, and that information will be transferred to the social network. If you do not want this data transfer to take place, please exit your social network session before entering our

websites or mobile applications, as it is not in our power to influence this data collection and transfer through social connectors.

If the user, through our official website in a social network, decides to publish and / or share texts, photos, videos, and other information and / or content, he will be the only responsible for ensuring that such content complies with the corresponding legal regulations.

In any case, we may remove from this website and from our pages in social networks, any content published by the user when we detect that the user has violated the legislation in force, and what is indicated in this privacy policy.

Social Networks are not directly hosted in our Services. Your interactions with them are governed by their policies and not ours. Please read the privacy policies of these social networks for detailed information about the collection and transfer of personal data, your rights, and your privacy settings.

- ## Third-party data

Concerning other people´s data, you should respect their privacy by taking special care when publishing their personal data. We remind you that, as a user, you can only provide and consent to the processing of your personal data, but not those of third parties, and that if you provide us with data of third parties you are making a transfer of personal data, being your responsibility to have the prior and express consent of those third parties to use and provide them to us, and you are responsible for informing them of the inclusion of their data in our files.

The publication of third party data without their consent may infringe, in addition to data protection regulations, the right to honor, privacy or their own image, rights whose protection is governed by the provisions of Organic Law 1/1982, of 5 May, on the civil protection of the right to honor, personal and family privacy and one´s own image.

- ## Purpose

The data can be processed for different purposes, for example:

1. If you are a client/supplier (current or potential), or an investigator, to maintain contact and communication with you, provide the requested services, or, if applicable, maintain the contractual relationship with you.

2. If you are a mere user of our website or the sender or recipient of an e-mail, to maintain contact and communication with you and manage the requests you make to us online.

3. If you provide us your data with your curriculum vitae or send us your curriculum, we will contact you and manage the selection processes that we carry out.

4. The identification data of our workers and/or researchers who authorize it can be included on our website, in the profiles that CIC energiGUNE has in any social network, as well as in any other type of support: brochures, magazines, dossiers and other stationery with the purpose of informing about our activities or promoting them, and the professional profile of the members of our team and being part of the Centre´s photographic/video memory.

- ## Retention period

We will keep the personal data as long as the person concerned does not request its deletion. Even if required, we may keep them for the time necessary and limit their processing, only to comply with the legal/contractual obligations to which we are subject and/or during the statutory periods foreseen for the prescription of any responsibilities on our part and/or the exercise or defense of claims deriving from the relationship maintained with the data subject.

- ## Legitimation

The legal basis that legitimizes us to process your data may be different.

On the one hand, it can be the legal relationship that connects us if you are a current client/supplier or researcher or the pre-contractual relationship of any kind between the parts if you are a potential client/supplier (for example, if you have requested information from us).

It can also be your consent if you have made an application to us through our website, in the case of being a mere user of the same, or if you have sent us your resume or are an attendee at one of our events. This consent is given to us in an unequivocal way when you provide us with your data online or offline, considering this contribution a clear affirmative act that manifests this consent. You may withdraw this consent at any time by sending us an e-mail to that effect to info@cicenergigune.com. Such withdrawal implies that we will not be able to provide you with the requested services or attend to your requests.

So can compliance with regulations that affect us, such as those on consumers and users.

It may also be in our legitimate interest to:

- To inform you about our activities, products, and/or services if we already have a previous contractual relationship. Otherwise, we will only send you this type of communication if you give us your consent by checking the option that is expressly included for this purpose in the corresponding forms. In any case, the electronic communications that we send you will include, in the communication itself, the option to stop receiving them in the future.
- To carry out an opinion and/or satisfaction surveys.

- ## Recipients

We inform you that the data you provide may be communicated to third parties for the fulfillment of purposes directly related to legitimate functions of transferor and transferee as:

1. To banks for the management of collections and payments.
2. To entities or bodies to whom there is a legal obligation to communicate data (e.g., tax authorities for the fulfillment of tax and duty obligations).
3. The curriculum data and the curriculum itself to the relevant entities, agencies and / or public or private companies, within collaboration programs, research and / or framework funding for economic development projects and competitiveness (as an example Ministry of Economy and Competitiveness of the Government of Spain, European Union agencies, Basque Government, Provincial Council of Alava, companies or public or private organizations...) within Framework Funding Programs for Economic Development Projects and Competitiveness, or research projects and / or collaboration in companies or entities for: the application for and justification of grants, as well as the management and monitoring of these programs and R+D+i research projects in which you are involved. The cost of research personnel may also be communicated to these bodies to justify the subsidy.

International transfers

In the event that we use U.S. suppliers, who may have access to personal data, for the purpose of providing services related to our business (hosting, housing, software as a service, remote backup, support services or computer maintenance, email managers, sending e-mails and e-mail marketing,) these companies may be different and vary over time but, in any case, we will choose companies that are members of the Privacy Shield agreement between the USA and the EU, or belong to countries that have been declared as countries with an adequate level of protection, which means that they are obliged to comply with requirements equivalent to the European ones in terms of data protection.

We may also make international transfers of data in case a researcher requests to carry out part of his or her research in another country. In any case, by accepting this data protection policy, you expressly and unequivocally authorize such international transfer of data to a country outside the European Economic Area and give your unequivocal consent to such transfer.

Rights

When appropriate, you may exercise your rights of access, rectification, suppression, limitation and opposition to the processing of your data, as well as the right not to be subject to decisions based only on the automated processing of your data, at the postal or e-mail address indicated at the beginning of this privacy policy; in both cases by submitting a written and signed request, attaching a copy of your ID card or passport or other valid document that identifies you. In case of modification of your data, you must notify it to the same address. This company declines all responsibility in case of not doing it.

- Right of access: You can ask us what personal data we are processing and even ask us for a copy of them.
- Right of rectification: You can ask us to correct inaccurate personal data or to complete those that are incomplete, including by presenting an additional statement.
- Right of withdrawal (right of cancellation): You can ask us to delete your personal data when they are no longer necessary for the purposes for which they were collected, you withdraw consent, there has been an unlawful treatment of them, or for compliance with a legal obligation.
- The right to limitation of treatment: You can ask us to limit the treatment of your data, in which case, we will only retain them for the exercise or defense of claims.
- Right to the portability of the data: You can ask us to send you (or to a third party that you indicate) your personal data in a structured format, of everyday use, and mechanically readable.
- Right of opposition: You can oppose the treatment of your data if such treatment is based on the legitimate interest of the person responsible for the file, or it is for advertising purposes.

Once received any of the previous requests, we will respond to you within the legal deadlines.

You can make any claim to the Spanish Data Protection Agency. If you want more information about the rights you can exercise and to request models of the forms for the exercise of your rights you can visit the web page of the Spanish Data Protection Agency, www.aepd.es

5.4 Annex 4 UGent's GDPR Policies

Ghent University processes personal data of more than 9,000 staff members, 42,000 students, various alumni, external partners, visitors or other groups involved in the education, scientific research, quality assurance and business operations provided by Ghent University.

At Ghent University this data is handled in a careful and responsible way to safeguard the personal data and information of all data subjects concerned.

- More information can be found in the privacy policy of Ghent University

Your personal data is protected

Ghent University takes the protection of privacy very seriously. That is why the Executive Council of Ghent University approved the Generic Code of Conduct for the processing of personal data and confidential information on 18 May 2018.

With this Generic Code of Conduct Ghent University ratifies its General Data Protection Policy. Central to this is the security, accuracy, care and responsibility of the processing of personal data and confidential information, in addition to ensuring compliance with the General Data Protection Regulation.

- More information about the Generic Code of Conduct for the processing of personal data and confidential information

Specific privacy information

For (prospective) students

In order to be able to fulfil its educational responsibilities and to provide high quality education to all students, Ghent University processes personal data of (prospective) students who wish to pursue a study programme or course of training at Ghent University, and who consequently register (online) or (pre-)register for the same.

These data are accurately and securely stored in a database of Ghent University. The attention of (prospective) students is drawn to this regulation at the time of registration, pre-registration and re-registration. They may always consult and change their personal privacy settings at any time using the web application available for this purpose.

- More information concerning the processing of your personal data as a (prospective) student

For researchers

Researchers affiliated to Ghent University may collect, process, analyse and manage personal data in connection with conducting scientific research. This may involve sensitive data (e.g. medical data, ethnicity/race, data relating to personal or sexual life, etc.), according to the nature of the research.

The general principles that must also be respected in relation to scientific research have been laid down in the Generic Code of Conduct for the processing of personal data and confidential information in force within Ghent University.

Personal data within Ghent University-Research must always be handled in conformity with the broader policy of Research Data Management. A focus in this policy is to ensure the collection, management and storage of research data in an ethical manner and with the requisite quality.

- More information concerning research and privacy

For alumni

As a former student of Ghent University you are one of our most important ambassadors, and we hope that you have taken the trouble to register yourself in the Ghent University alumni database.

Your data will only be used in connection with alumni associations relating to data and membership management, sending the alumni newsletter and other faculty or study programme-related applications.

As Ghent University alumni, you may always consult your data and privacy preferences and even modify the same if necessary, using your own registration/login.

- More information about alumni at Ghent University.
- Please contact alumni@ugent.be or the Data Protection Officer via privacy@ugent.be by e-mail in case you have any questions, comments or suggestions about the processing of your personal data in connection with Ghent University alumni associations.

For contributors

Just like your support, your personal data as a contributor are also close to the heart of Ghent University.

The personal data of (potential) contributors and sympathisers are stored and processed by Ghent University in order to enable their close monitoring, registration, and for the purpose of issuing a tax certificate (proof of payment issued as per Section 145[33], § 1(2), of the Income Tax Code 1992).

Ghent University processes the following categories of personal data

- Identification data such as surname, first name, address, date of birth
- Financial data such as the account number and the donation amount
- Contact details such as e-mail address

These personal data are processed to enable the issue of tax certificates and to promote the legitimate interests of Ghent University. This is done by creating and optimising a relational bond and a university community, in order thereby to contribute to the social relevance of donations for research and education.

The personal data of the contributors are not disclosed to third parties (except to government agencies for legal or fiscal reasons).

The explicit consent of the concerned contributors shall be taken before making any public disclosure of a contributor's personal data (e.g. to express gratitude on Ghent University website).

- More information about fundraising or donating to Ghent University
- Please contact universiteitsfonds@ugent.be by e-mail or the Data Protection Officer via privacy@ugent.be in case you have any questions, comments or suggestions concerning the processing of your personal data for fundraising by Ghent University.

Contact

In most cases, Ghent University, legally represented by its rector, bears ultimate responsibility for the processing of personal data at Ghent University.

Ghent University has therefore appointed a Data Protection Officer who coordinates the further development and implementation of Ghent University's policy on the processing and protection of personal data and confidential information.

Data Protection Officer

Please contact the Data Protection Officer in case you have any questions, comments or suggestions concerning the various rights and obligations relating to privacy, or if you believe that Ghent University is processing your personal data wrongfully and/or improperly:

Hanne Elsen
Department of Administrative Affairs
Sint-Pietersnieuwstraat 25
9000 Ghent
privacy@ugent.be

Additional information

Ghent University may request additional information in order to assess the well-foundedness of such a request or to verify the identity of a person making the same.

Ghent University reserves the right not to comply with such requests, provided it states the grounds for the same. This may apply, for example, if such a request is manifestly unfounded or excessive in nature.

Complaints

If, after processing a request or complaint, you believe that insufficient action has been taken, you may contact the Flemish Supervisor using the following details:

Flemish Supervisory Committee for the processing of personal data
Koning Albert II-laan 15
1210 Brussels
Telephone: +32 (0)2 553 50 47
Contact

5.5 Annex 5 LEITAT's GDPR Policies

POLÍTICA DE PRIVACIDAD
AT-DOC0026 Revisión: 0 Página: 1 de 2

LEITAT
managing technologies

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS

Responsable del tratamiento	LEITAT – TECHNOLOGICAL CENTER (ACONDICIONAMIENTO TARRASENSE), en adelante, LEITAT
Finalidad	-Gestión de los servicios contratados; -Tratamiento con finalidades comerciales, envío de ofertas, información y propuestas comerciales.
Legitimación	Consentimiento del interesado, a excepción de determinados supuestos en los que exista interés legítimo.
Destinatarios	Sus datos serán tratados exclusivamente por LEITAT, a excepción de aquellos casos en los que la comunicación de sus datos a terceros sea necesaria para poder cumplimentar el fin directamente relacionado con el servicio contratado.
Conservación de los datos	Hasta la finalización del servicio o exista obligación legal.
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional. Presentar una reclamación ante Autoridad de Control (www.agpd.es).
Información adicional	Puede consultar la información adicional y detallada sobre la Protección de Datos en el siguiente apartado.

INFORMACIÓN ADICIONAL SOBRE PROTECCIÓN DE DATOS

¿Quién es el responsable de tratamiento de tus datos?	
Identidad	LEITAT - TECHNOLOGICAL CENTER (ACONDICIONAMIENTO TARRASENSE), en adelante, LEITAT CIF: G-08360232 Inscrita en el Registro de Asociaciones de Barcelona Número 16
Dirección postal	C/de la Innovació número 2, 08225, Terrassa (Barcelona),
Teléfono	93.788.23.00
e-mail	legal@leitat.org
Delegado de Protección de Datos	Badia)Advocats, Andreu Alonso aalonso@badia-adv.com
¿Con que finalidad tratamos sus datos?	
• Gestión de los servicios contratados y realización de encuestas de opinión y satisfacción; • Envío de comunicaciones comerciales y promocionales.	
¿Cuál es la legitimación del tratamiento de sus datos?	
• Relación contractual entre LEITAT y el usuario en el momento de la ejecución del servicio contratado. Para llevar a cabo el servicio contratado es obligatorio que nos facilite los datos personales que se le pidan. Si no nos facilita sus datos personales, el servicio contratado no podrá ser efectuado. • Su consentimiento libre, específico, informado, inequívoco.	
¿A qué destinatarios comunicamos sus datos?	
Sus datos serán tratados exclusivamente por LEITAT con la siguiente excepción: los datos que nos proporcione podrán ser comunicados a terceras entidades para el cumplimiento de fines directamente relacionados con el servicio contratado arriba indicados entre LEITAT y el cedente de los datos, como a las entidades u organismos a los que exista obligación legal. No se producirán transferencias a terceros países fuera de la Unión Europea sin que medie su consentimiento.	
¿Cuánto tiempo conservamos sus datos personales?	
Los datos personales que nos facilite se conservarán mientras haya un interés mutuo para mantener la finalidad del tratamiento, o cuando sea necesario conservarlas por razón de obligaciones legales. Cuando la conservación ya no sea necesaria, se suprimirán con las medidas de Seguridad adecuadas para garantizar la seudonimización de los datos o su destrucción total.	

Revisado por:	Aprobado por:
OLGA BONASTRE PEREMATEU DIREC. DE CALIDAD, MEDIOAMBIENTE Y PRL 26-02-2020	CARLES GIMENO GRANE DIREC. SEGURIDAD EN PERSONAS Y SISTEMAS 26-02-2020

LEITAT
managing technologies

POLÍTICA DE PRIVACIDAD
AT-DOC0026 Revisión: 0 Página: 2 de 2

¿Cuáles son sus derechos cuando nos facilita sus datos personales?

- Derecho a retirar el consentimiento en cualquier momento;
- Derecho a acceder, rectificar y suprimir los datos;
- Derecho de limitación del uso u oposición del tratamiento de datos;
- Derecho a presentar una reclamación ante la Autoridad de Control (www.agpd.es), si considera que el tratamiento no se ajusta a la normativa vigente.

Descargue aquí el Modelo de Ejercicio de Derechos.

Datos de contacto para ejercer sus derechos:

C/de la Innovació número 2, 08225, Terrassa (Barcelona),
DPO: Badia)Advocats, Andreu Alonso aalonso@badia-adv.com

Revisado por:	Aprobado por:
OLGA BONASTRE PEREMATEU DIREC. DE CALIDAD, MEDIOAMBIENTE Y PRL 26-02-2020	CARLES GIMENO GRANE DIREC. SEGURIDAD EN PERSONAS Y SISTEMAS 26-02-2020

5.6 Annex 6 TORRECID's GDPR Policies

TORRECID

CERTIFICATE OF GUARANTEE OF COMPLIANCE WITH PERSONAL DATA PROTECTION

Hereby, on behalf of Torrecid Group and as its Data Protection Officer (GDPO),

CERTIFIES

That in accordance with the provisions of Regulation (EU) 2016/679 of 27 April (GDPR), all Torrecid Group companies, S.A. are complying with all the provisions of the GDPR for the processing of personal data of its responsibility, and manifestly with the principles described in Article 5 of the GDPR, by which they are treated in a lawful, fair and transparent manner in relation to the data subject and suitable, relevant and limited to what is necessary in relation to the purposes for which they are processed.

That Torrecid assumes its obligation to respect the privacy rights of individuals and undertakes to responsibly treat personal information in compliance with applicable legislation on privacy protection and data security. That is why Torrecid conducts all its business in compliance with the aforementioned legislation.

That Torrecid guarantees that appropriate technical and organisational policies have been implemented to apply the security measures established by Article 32 of the GDPR in order to protect the rights and freedoms of the Data Subjects and has communicated the appropriate information for them to be able to exercise them.

Torrecid Group undertakes to process personal data, regardless of the origin of the interested parties (residing in the European Union or in a third country), in accordance with the provisions of the aforementioned internal regulations.

From all this, I certify that TORRECID, S.A. and all the subsidiaries and investee companies of the Torrecid Group, and others with which any company of the Torrecid Group has signed collaboration agreements, comply with the obligations regarding compliance with the Regulation (EU) 2016/679.

GDPR Compliance 1 / 2

Specifically and for the purpose of this certificate, the measures established regarding information security are detailed, without this list being exhaustive of all the measures, but serving as an indicator of them:

- Training in Information Security and its treatment
- Security of information about third parties and internal personnel
- Internal information system - complaints and suggestions protocol
- Risk assessments and personal data protection audit reports.
- Action protocols - treatment - control and access to information.
- Mandatory data protection decalogue for employees
- Record of Activities and Security Measures
- Contracts and clauses to guarantee the security of information

Alcora, 09 August 2023

Alejandro Ros Igual
DPO - Data Protection Officer Torrecid Group

5.7 Annex 7 LOMARTOV's GDPR Policies

5.8 Annex 8 CALDERYS's GDPR Policies

Data Processing Agreement

Between

Calderys France SAS, a French entity having its registered office at XXXXXXXXXX (the "**Controller**");

and

XXXXXXXX (the "**Processor**");

and

each also referred to as "**Party**" or together referred to as "**Parties**" of this Agreement.

(A) The Controller has appointed XXXXXXXXX as its Service Provider under a separate Services Agreement which entails the processing of personal data in the name and on behalf the Controller by the Processor.

(B) In order to ensure compliance with the data processing obligations pursuant to the Data Protection Laws (as defined hereunder), the Controller and the Processor hereby agree as follows:

1. Definitions

For the purposes of this Data Processing Agreement, the following terms shall bear the meaning defined hereunder:

Data Protection Laws: means the French data protection act 78-17 of 6 January 1978, as last revised, the Regulation 2016/679 of 27 April 2016 ("GDPR"), as well as any laws relating to data protection and privacy substantially amending, replacing, supplementing or superseding the GDPR, including where applicable, statutes, decisions, guidelines, guidance notes from time to time by courts, any data protection supervisory authority and other applicable authorities.

If not defined otherwise in this Data Processing Agreement, the terms "personal data", "processing", "personal data breach" and "supervisory authority" shall have the meaning given to them by Article 4 of the GDPR. Other capitalized terms defined in this Data Processing Agreement shall bear the meaning given to them under this Data Processing Agreement.

2. Subject matter

a. The Processor shall store and process, on behalf of the Controller, the data, including personal data in the scope and for the Purposes, as detailed in **Annexe I** (the personal data

processed in the context of the Purposes and listed in **Annex I** hereinafter "**Personal Data**"). The Personal Data will be provided by the Controller to Processor. The Parties may choose to amend **Annexe I** by way of a written amendment to this Data Processing Agreement to reduce or expand the Purposes and/or scope and types of Personal Data processed in the context thereof.

3. Instructions of the Controller

3.1 The Processor shall process the Personal Data provided by the Controller solely in accordance with the Controller's legitimate and documented instructions, and the provisions contained in this Agreement, and as amended by the Controller from time to time by way of a written amendment to this Data Processing Agreement. The Controller in particular may give instructions regarding the type, extent and method of the data processing, within the limits of the technology used.

3.2 On the day of the signature of this DPA, the Processor does not plan to resort to means of processing located outside the EEA. In the event that the Processor intends to transfer Personal Data outside the EEA, it must first inform the Controller and seek its agreement. Should such agreement be given by the Controller, the Processor will implement mechanisms in order to ensure that a level of data protection similar to that of the Data Protection Laws is safeguarded (article 46 of the GDPR, in particular by concluding data transfer agreements based on the respective EU-model clauses for data transfers to third-countries) if a transfer is made to a country which does not offer an adequate protection. The Processor will carry out a risk assessment before relying on a transfer tool to make a data transfer outside the European Economic Area, according to the decisions of the European Court of Justice (Schrems II (case C-311/18) dated July 16, 2020). The Processor will take additional measures when the risk assessment reveals that there are elements that may undermine the effectiveness of the appropriate safeguards provided by the transfer instrument referred to in article 46 of the GDPR.

3.3 If the Processor is of the opinion that an instruction infringes applicable Data Protection Laws, it shall immediately notify the Controller unless required to do so by Union or Member State law to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the processing of personal data.

3.4 The Processor confirms that he is aware of the reporting and notification obligations with respect to personal data breaches to supervisory authorities or data subjects and with respect to data subject rights, in accordance with Data Protection Laws, including the requirements in terms of timing and subject matter. Consequently, the Processor shall immediately notify the Controller at

hand of such events without regard to the cause. The Processor shall take, and ensure any Sub-Processor is under a contractual obligation to take, the appropriate technical and organisational measures in order to secure the concerned Personal Data and to mitigate any potential negative effects on data subjects. The Processor shall assist the Controller with respect to notification and reporting obligations of each Controller under the Data Protection Laws. The Processor shall document any personal data breach, its effects and the remedial action taken, in accordance with the Data Protection Laws. The Processor shall release such documentation to the Controller upon request without undue delay.

4. Obligations of the Processor

4.1 Processor shall structure its internal corporate organisation to ensure compliance with the specific requirements of the Data Protection Laws. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the Agreement and the Data Protection Laws.

4.2 The Processor shall assist the Controller in ensuring compliance with the obligations in articles 32 to 36 of the GDPR.

4.3 Processor shall take, and ensure any Sub-Processor is under a contractual obligation to take, the appropriate technical and organisational measures to adequately protect the Personal Data against misuse and loss in accordance with the requirements of Data Protection Laws, as described in **Annex II**. This includes in particular the following:

4.3.1 The prevention of unauthorised persons from gaining access to data processing systems (physical access control),

4.3.2 The prevention of data processing systems from being used without authorisation (logical access control),

4.3.3 Ensuring that persons entitled to use a data processing system gain access only to such Personal Data strictly necessary for implementing the Purposes and as they are entitled to accessing in accordance with their access rights, and that, in the course of processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorisation (data access control),

4.3.4 Ensuring that Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control),

4.3.5 Ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from data processing systems, (entry control),

4.3.6 Ensuring that Personal Data processed are processed solely in accordance with the Controller's instructions (control of instructions),

4.3.7 Ensuring that Personal Data are protected against accidental or unlawful destruction, alteration, unauthorised disclosure or access to the Personal Data or loss (availability control),

4.3.8 Ensuring that Personal Data collected for different purposes can be processed separately (separation control),

4.3.9 Ensuring that Personal Data can be pseudonymised and encrypted as appropriate having regards to the nature, scope context and purposes of the processing of Personal Data as well as the risks and varying likelihood and severity for the rights and freedoms of data subjects,

4.3.10 Ensuring that the ongoing confidentiality, integrity, availability and resilience of processing systems and services is permanently secured,

4.3.11 Ensuring that the availability and access to Personal Data can be restored in a timely manner in the event of a physical or technical incident,

4.3.12 Ensuring that a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing is complied.

4.4 A measure as referred to in section 4.3.1 to 4.3.12 above shall be in particular, but shall not be limited to, the use of state-of-the-art encryption technology. The Processor shall ensure the continued testing, assessing and evaluating as well as adjusting and updating of this data protection and security concept. Changes need to be agreed upon in writing upfront. Processor shall ensure that any of its personnel entrusted with processing Personal Data have entered into suitable confidentiality undertakings to maintain confidentiality of the Personal Data. The undertakings shall continue after the termination of the activities carried-out by the Processor under this Data Processing Agreement.

4.5 Processor shall, without undue delay, inform the Controller in case of a serious interruption of operations, suspicion of personal data breach, and any other irregularity in processing the Personal Data. The notification of the personal data breach shall at least contain:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

4.6 Processor shall, without undue delay, inform the Controller on controls/checks and other measures conducted by a data protection authority, unless the Processor is prohibited to do so under applicable statutory law.

4.7 Processor shall conduct regular control checks, including investigations and audits, concerning its compliance with its obligations towards data protection and security hereunder. In addition, Processor shall conduct regular control checks regarding the compliance of any Sub-Processor with the Data Protection Laws.

4.8 The Controller shall retain title as to any data carrier media provided to Processor as well as any copies or reproductions thereof. Processor shall store such media safely and protect them against unauthorized access by third parties in accordance with this Data Processing Agreement. Processor shall be obliged to securely delete any test and scrap material based on an instruction issued by each Controller on a case-by-case basis. Where a Controller decides so or, subject to confidentiality, when such Controller terminates its participation to this Data Processing Agreement, for any reason whatsoever, Processor shall hand over such material to said Controller or store it on Controller's behalf.

4.9 Processor shall appoint a data protection officer where mandated by the Data Protection Laws, or appoint a person in charge of handling data protection issues within Processors' organisation. The Processor shall provide the contact information of such individual to the Controller for direct support.

4.10 The Processor shall maintain a record of processing activities which complies with Data Protection Laws. The Processor shall make the record available to the supervisory authorities on request and inform the Controller about any such requests without undue delay. The Processor may only disclose Personal Data information to the service providers (Sub-Processors) and other third parties as necessary for the achievement of the Purposes.

5. Responsibility of the Controller

5.1 The Controller remains responsible for the compliance of the processing of Personal Data in the context of this Data Processing Agreement with Data Protection Laws and the Controller is solely responsible for the protection of the data subject's rights pursuant to Data Protection Laws. The Controller is also solely responsible for providing adequate information to data subjects about the data processing hereunder and, if necessary, obtaining their consent thereto.

5.2 In case that data subjects assert their rights, e.g. to information, correction, erasure, blocking or deletion, the Controller shall inform data subjects that they may exercise these rights solely vis-à-vis the Controller. Said rights shall not be asserted against the Processor. If a data subject approaches the Processor directly with a request regarding his/her Personal Data, Processor shall immediately forward the request to the Controller at hand, which will handle and address such request in accordance with the Data Protection Laws. To the extent required by the Data Protection Laws, the Processor shall assist the Controller by appropriate technical and organisational measures for the fulfilment of the Controller's obligation to respond to data subject requests for exercising their rights under Data Protection Laws.

5.3 The Controller is the sole responsible for ensuring the quality of any Personal Data it sends to Processor or to which it grants Processor access. The Controller holds all rights in relation to the Data.

5.4 The Controller shall, upon termination or expiration of this Data Processing Agreement and by way of issuing a written instruction, stipulate the measures to (i) return data carrier media or, at Controller's discretion, (ii) return Personal Data processed and delete existing copies thereof or (ii) delete Personal Data Processor may still hold. Processor will comply with such instructions without undue delay. In any event, Processor may still store Personal Data further to that date, if and to the extent European Union or Member State law requires storage of such Personal Data by Processor.

6. Inspection rights of the Controller

6.1 The Controller is entitled to inspect and audit the technical and organisational measures and the data processing work flows of the Processor at reasonable intervals and in any event not more than once a year, upon reasonable prior written notice and during regular business hours, without affecting the Processor's usual course of business, in order to verify compliance by the Processor with the terms and conditions of this Data Processing Agreement and in particular with the obligations on technical and organizational measures mentioned in Section 4.3 of this Data

Processing Agreement. For such purpose, Controller may collect voluntary disclosures from Processor.

6.2 Processor shall, upon Controller's written request and within a reasonable period of time, provide Controller with all information necessary for such audit.

6.3 Controller and Processor shall make the results of the audits available to the competent supervisory authority/ies on request.

7. Sub-processors

7.1 The Controller hereby authorizes the Processor to engage or replace Sub-Processors listed in **Annex III**, from an agreed list, to process Personal Data to achieve the Purposes under this Data Processing Agreement. The Processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object. If the Controller objects a change of a Sub-Processor, the Processor will cease to provide all or part of the services that require the assistance of said Sub-Processor to the Controller at hand.

7.2 The engagement or replacement of Sub-Processors established outside the EEA, or inside the EEA but not belonging to Processor's group of companies, is also generally permitted by Controller, subject to Processor complying with sections 3.2 and 7.1 of this Data Processing Agreement.

7.3 Where Processor engages Sub-Processors, Processor shall be obliged to pass on Processor's contractual obligations hereunder to such Sub-Processors. The Processor shall ensure that the Sub-Processors comply with the obligations to which the Processor is subject pursuant to this Data Processing Agreement and to Data Protection Laws. The Processor shall provide a copy of such sub-processors' agreements and any subsequent amendments to the Controller. Where a sub-processor outside the EEA is used pursuant to sections 7.1 and 7.2 above, Processor must take additional measures to ensure that an adequate level of data protection in accordance with Data Protection Laws is in place.

7.4 The Processor shall be liable to the Controller for any acts or omissions of Sub-Processors resulting in a violation of the Processor's obligations under this Data Processing Agreement. The Processor shall notify the Controller of any failure by the Sub-Processor to fulfil its contractual obligations.

8. Term

8.1 This Data Processing Agreement and any processing of Personal Data in the context thereof is effective as of its signature date and shall remain in force for the duration of the separate Services Agreement.

8.2 Each Party's right to terminate this Data Processing Agreement for reason remains unaffected and does not affect the validity of the Data Processing Agreement. Either Party may in particular terminate this Data Processing Agreement by giving to the other Party written notice if the other Party has breached any of its material obligations under this Agreement and failed to cure such default within a reasonable period of time upon receipt of a respective prior written notice. In the event the Processor terminates its participation to the Data Processing Agreement, any processing of Personal Data in the context of this Data Processing Agreement shall be terminated immediately.

8.3 The material obligations of this Agreement will continue to apply irrelevant of the termination until the Data have been returned to Controller or deleted by the Processor, in accordance with section 5.4 above.

9. Miscellaneous

9.1 Amendments to this Data Processing Agreement shall be made in writing. This also applies to the form requirement in this paragraph.

9.2 Should a provision of this Data Processing Agreement be held invalid by a Court or Authority having jurisdiction, the validity of the other provisions of this Agreement shall remain unaffected hereby. The Parties agree that in the place of the invalid provision, a legally permitted provision shall apply which comes closest to what the Parties would have agreed if they had taken the partial invalidity into consideration.

9.3 The Agreement represents and contains the full and complete agreement between the Parties with respect to the subject matter hereof and supersedes and replaces all prior and contemporaneous agreements and understandings between the Parties with respect to such subject matter.

9.4 This Agreement shall exclusively be governed by the laws of France. Both Parties hereby submit to the exclusive jurisdiction of the courts of Paris, France for any disputes and proceedings arising out of or in connection with this Agreement.

9.5 The Agreement may be executed in two or more counterparts, and may be executed by way of electronic signature, and if so, shall be considered as a handwritten signature on this agreement. The Parties agree that the electronic signature expresses the consent for this Agreement to be legally binding to the Parties and to serve as evidence on the same account as a hand-signed paper document.

Calderys (the Controller

ANNEX I. DESCRIPTION OF TRANSFER

Purpose of the transfer :

The frequency of the transfer :

The personal data will be retained for the duration specified between the data subject and the controller,

Tool used :

CLIENT DATA

Purpose of the transfer :

The frequency of the transfer :

The personal data will be retained for the duration specified between the data subject and the controller.

Tool used :

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The Processor undertakes to institute and maintain the following data protection measures (the relevant measures are marked below by a tick in the respective box):

1. Access control of persons

The Processor shall implement suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment until the Personal Data transferred by the Controller are processed.

This shall be accomplished by:

☐ Establishing access authorizations for employees and third parties, including the respective documentations;

☐ Code card passes;

☐ Restrictions on keys;

☐ Regulations for third parties;

☐ Regulations on key codes;

☐ Identification of the persons having access authority;

☐ Security alarm system or other appropriate security measures even after the working time;

☐ Securing the decentralized data processing equipment and personal computers;

☐ Protection and restriction of access path.

2. Access control to Personal Data

The Processor commits that the persons entitled to use the data processing system are only able to access the Personal Data within the scope and to the extent covered by the respective access permission (authorization).

This shall be accomplished by:

☐ Locking of terminals;

☐ Allocation of individual terminals and/or terminal user and identification characteristics exclusive to specific functions;

☐ Functional and/or time restricted use of terminals and/or terminal users and identification characteristics;

☐ Regulations for user authorization;

☐ Obligation to comply with data secrecy;

☐ User codes for Personal Data and programs;

☐ Coding routines for files;

☐ Differentiated access regulations (e. g. partial blocking);

☐ Regulations for the organisation of files;

☐ Logging and analysis of use of the files;

☐ Special control regarding the application of help programs as far as they are able to evade security measures;

☐ Controlled destruction of data media;

☐ Work instructions for templates for the registration of Personal Data;

☐ Checking, adjustment and controlling systems;

☐ Processes for the checking and release of programs.

3. User Control

The Processor shall implement suitable measures to prevent its data processing systems from being used by unauthorized persons by means of data transmission equipment. In addition, the Processor shall implement suitable measures to prevent unauthorized reading, copying, alteration or removal of the data media, unauthorized input into memory, reading, alteration or deletion of the stored Personal Data.
This shall be accomplished by:

☐ Authorization concept;
☐ Terminal with access user key;
☐ Identification of the terminal and / or the terminal user to the system of the Processor;
☐ Automatic turn-off of the user ID when several erroneous passwords where entered;
☐ Log file of events (monitoring of break-in attempts);
☐ Issuing and safeguarding the identification codes;
☐ Dedication of individual terminals and/or terminal users;
☐ Identification characteristics exclusive to specific functions;
☐ Authentication of the authorized personnel;
☐ Protective measures for the data input into memory as well as for the reading, blocking and deletion of stored Personal Data;
☐ Use of encryption for critical security files;
☐ Specific access rules for procedures, control cards, process control methods, program cataloguing authorization;
☐ Guidelines for data file organisation;
☐ Keeping records of data file use;
☐ Separation of production and test environment for libraries and data files;
☐ Providing that entries to data processing facilities (rooms, housing, computer hardware and related equipment) are capable of being locked;
☐ Automatic log-off of user IDs that have not been used for a substantial period of time;
☐ Designating the areas in which data media may / must be located;
☐ Designating the persons in such areas for authorized remove of data media;
☐ Controlling the removal of data media;
☐ Securing the areas in which data media are located;
☐ Release of data media only to authorized persons;
☐ Control of files, controlled and documented destruction of data media;
☐ Policies controlling the production of backup copies.

4. Transmission control

The Processor shall be obliged to enable the verification and tracing of the locations/destinations to which the data subject's Personal Data are transferred by the utilization of the Processor's data communication equipment/devices.
This shall be accomplished by:

☐ Authentification of the authorized personal;

☐ In-house verification requirements (four-eye principle);
☐ Designating the areas in which data media may / must be located;
☐ Controlling the removal of data media;
☐ Designating the persons in such areas who are authorized to remove data media;
☐ Control of files;
☐ Locking of confidential data media;
☐ Security lockers;
☐ Prohibition of taking bags etc. within the secure area;
☐ Control of destruction of data media;
☐ Policies controlling the production of backup copies;
☐ Documentation of the transfer programs;
☐ Documentation of the retrieval and transmission programs;
☐ Documentation of the remote locations/destinations to which a transmission is intended and the transmissions path (logical path);
☐ Authorization policy;
☐ Encryption of the Data for online transmission or transport by means of data carries (tapes and cartouches);
☐ Monitoring of the completeness and correctness of the transfer of Data (end to end check);
☐ Encryption;
☐ Courier services, personal pickup, accomplishing of the transport;
☐ Control of plausibility;
☐ Control of completeness and correctness;
☐ Deletion of remaining Personal Data before change of data media.

5. Input Control

The Processor shall provide for the retroactive ability to review and determine the time and the point of the data subject's Personal Data entry into the Processor's data processing system.
This shall be accomplished by:
☐ Proof of Processor's organisation of the input authorization;
☐ Electronic recording of entries;
☐ Electronic recording of data processing, in particular usage of Data.

6. Organisation control

The Processor shall maintain its internal organisation in a manner that meets the requirements of this Agreement.
This shall be accomplished by:

☐ Internal data processing policies and procedures, guidelines, work instructions, process descriptions and regulations for programming, testing and release, insofar as they relate to the Personal Data transferred by the Controller;

☐ Formulation of a data security concept;

☐ Industry standard system and program examination;

☐ Formulation of an emergency plan (backup contingency plan).

7. Instructional control

The Data transferred by the Controller to the Processor may only be processed in accordance with the instructions of the Controller.
This shall be accomplished by:

☐ Binding policies and procedures for the Processor's employees;

☐ Upon request, access will be granted to those of the Controller's employees and agents who are responsible for monitoring the Processor's compliance with this Agreement.

8. Control of separation of Personal Data

The Processor shall implement suitable measures to allow the separate processing of Personal Data which have been collected for different purposes.
This shall be accomplished by:

☐ Storage of the Personal Data in separated data collectors (physical separation);

☐ Authorization policy (logical separation);

☐ Separation of the Personal Data, which have been stored under an alias (pseudonym) from the original Personal Data.

ANNEX III – LIST OF SUB-PROCESSORS

5.9 Annex 9 ALCOA's GDPR Policies

Alcoa Online Privacy Notice

We at Alcoa Corporation ("Alcoa") respect your concerns about privacy. This Online Privacy Policy Notice applies to Alcoa.com and other external Alcoa websites that link to this Notice (the "Sites"). This Privacy Policy applies to all personal data We collect or process about you in relation to the use of Alcoa.com and other Sites.

'**Personal Data**' means any information relating to an identified or identifiable natural person 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.

This Notice describes the types of personal data we collect on the Sites, how we use this information, with whom we share it and the choices available to users of our Sites regarding our use of this information. We also describe the measures we take to protect the security of this information and how users can contact us about our privacy practices. Certain of the Sites may provide additional detail about privacy practices specific to those Sites. Internal company policies and procedures govern Alcoa's internal networks and systems and the processing of personal information relating to employees and other authorized Alcoa network users. will collect and subsequently process the personal data as the data controller. You may contact Us at:

Alcoa Corporation
Attn: Corporate Communications/Privacy
201 Isabella Street
Suite 500
Pittsburgh, PA 15212
412-315-2900
editor@alcoa.com

Data Protection Officer Contact: AlcoaDPO@alcoa.com

1. **WHAT PERSONAL DATA DO WE COLLECT**

   We will collect personal data about you from a variety of sources, including information we collect from you directly when you contact us on our Sites.

   The categories of personal data that We collect directly from you include:

   1. contact information (such as name, postal address, telephone number and email address);
   2. employment information (such as title, division and employer);
   3. login credentials for the Sites;
   4. other personal information submitted by current or prospective suppliers and subcontractors, such as Social Security number, diversity-related information (such as ethnicity), federal tax ID number, disability status, and civil and criminal court history;
   5. other personal information submitted by job applicants, such as a résumé or C.V., work authorization information, salary history, education history, information about security clearances, citizenship information and, for jobs with U.S.-based Alcoa entities, ethnicity, race and gender;
   6. other personal information found in content that users provide; and

7. Information We collect automatically from you [describe, e.g. data collected using cookies and other device identifying technologies. When you use our Sites, we may collect certain information by automated means, using technologies such as cookies, web server logs, web beacons and JavaScript.

   Cookies are files that websites send to your computer or other Internet-connected device to uniquely identify your browser or to store information or settings on your device. Our Sites may use cookies (such as HTTP and HTML5 cookies) and Flash cookies, as well as other types of local storage (such as browser-based or plugin-based local storage). Your browser may tell you how to be notified when you receive certain types of cookies and how to restrict or disable certain cookies. You also may be able to delete your Flash cookies or adjust your Flash cookie settings by visiting the Adobe Flash Website Storage Settings Panel and Global Storage Settings Panel:

   Please note, however, that without cookies you may not be able to use all of the features of our Sites or other websites and online services.

   In conjunction with gathering information through cookies, our web servers may log information such as your device type, operating system type, browser type, domain, and other system settings, as well as the language your system uses and the country and time zone where your device is located. We also may record information such as the address of the web page that referred you to our Sites and the IP address of the device you use to connect to our Sites. We also may log information about your interaction with the Sites, such as which pages you visit. We may place tags on our web pages called "web beacons," which are small files that link web pages to particular web servers and their cookies.

   We may use third-party web analytics services on our Sites, such as those of Google Analytics, Adobe Omniture, ScorecardResearch and DocAve Analytics. These service providers help us analyze how users use the Sites. The information collected for this purpose (including your IP address and other information collected by automated means) will be disclosed to or collected directly by these service providers. To learn more about how to opt out of these third-party web analytic service providers' activities, click the relevant link below:

   Google Analytics

   Adobe Omniture

   ScorecardResearch

   DocAve Analytics

   Both we and others (such as our service providers and advertising networks) may collect personal information about our visitors' online activities, over time and across third-party websites. Our Sites are not designed to respond to "do not track" signals from browsers.

   The providers of other third-party plug-ins on our Sites, such as embedded videos and social sharing tools, may use automated means to collect information regarding your use of the Sites and your interactions with the plug-ins. This information is subject to the privacy policies or notices of the third-party plug-in providers and is not subject to Alcoa's Online Privacy Notice.

2. **HOW WE USE YOUR PERSONAL DATA AND ON WHAT LEGAL BASIS**

We use and subsequently process personal data We collect about you on the following legal basis, and for the purposes identified below:

1. We will process your personal data **on the basis of our legitimate interest**, for the following purposes:

    - Provide and personalize our Services;
    - To manage our Website;
    - To deal with your enquiries and requests;
    - To protect the security and/or integrity of our Website and IT infrastructure;
    - To understand how you use our services and to enable Us to improve and further develop the features, performance and support available on our Website, which may entail the provision of anonymous statistical information about our visitors (however, without it being used to identify any individual user);
    - As mentioned in Section 5 of this Privacy Policy, among other, for disclosures to any of our employees, officers, agents, business partners, affiliates of the Alcoa Group, who process the personal data for the purposes set forth in this Privacy Policy;
    - To allow third party service providers and vendors engaged by Alcoa to access the personal data in order to provide Us with the services required to fulfill the purposes set forth in this Privacy Policy;
    - For any disclosures to third parties required as part of due diligence processes in the context of corporate restructuring operations in which We may participate, in line with [Section 5(d)] of this Privacy Policy; and

    Where Alcoa processes personal data in fulfillment of its own legitimate interests, it shall always balance such interests against the data subjects´ fundamental rights and freedoms, and implement robust safeguards in view of ensuring that their privacy is protected accordingly. You may obtain information on such balancing test upon your request.

2. We will process your personal data for the following purposes, provided that **you have granted your prior consent**:

    - To contact you with electronic newsletters and/or promotional e-mails relating to products and services offered by Us, unless you have expressly manifested your desire to opt out of such marketing communications, or We are otherwise legally prevented from doing so;
    - For any other purpose disclosed to you at the time you provide Us with your personal data, to the extent that you have granted Us your prior consent to that particular processing. For example, We will obtain your consent to collect and use certain types of personal data when we are required to do so by law (e.g. in relation to our direct marketing activities, Cookies and Tracking Technologies, or when We process sensitive personal data); and

If We ask for your consent to process your personal data, you may withdraw your consent at any time by **contacting us**.

We will also process your personal data in order to ensure an optimum level of compliance with the applicable legal obligations to which Alcoa is subject, and cooperate with regulators and law enforcement bodies where necessary, in line with [Section 5] of this Privacy Policy:

- To disclose your personal data and other complementary information subject to requests received from authorities and/or bodies with compelling power, as required by the applicable laws or by law enforcement officers invested with such powers.

  Compliance with the aforementioned legal obligations to which Alcoa is subject is required by various types of legislation, laws, regulations and rules.

3. WHAT RIGHTS DO YOU HAVE OVER YOUR PERSONAL DATA

You have certain rights regarding your personal data, subject to local law. These include the following rights:

- To know how We are processing your personal data and to access your personal data held by Alcoa and its affiliates, where applicable;
- To request the rectification of inaccurate or incomplete personal data;
- To request the erasure of your personal data when such data is no longer necessary for the initial purposes for which it has been initially collected, in accordance with applicable law;
- To restrict our processing of your personal data, under certain circumstances (in which case We will only retain the personal data for the exercise and/or defense of Alcoa's rights);
- To object to our processing of your personal data, having regard to the given circumstances and for reasons related to their particular situation (in which case We will only retain the personal data for imperative legitimate reasons or the exercise and/or defense of Alcoa's rights);
- This includes the right to object, at any time, for reasons related to your particular situation, to our processing of your personal data based on our legitimate interests or those of a third party, in which case We will cease in processing your personal data unless We are able to rely on legitimate reasons to do so.
- To request the portability of your personal data, which will allow you to obtain and reuse the personal data in a usable electronic format for your own purposes and across different services without hindrance to usability, including its transmission to another third party; and
- To withdraw the consent you may have granted to a specific processing, at any time.

We encourage you to contact us to update or correct your information if it changes or if the personal data We hold about you is inaccurate.

We will contact you if we need additional information from you in order to honor your requests.

Alcoa is committed to protecting your personal data as described in this policy, and as required by applicable laws. Should you have any queries or intention of requesting additional information on how to exercise your rights or to effectively submit such a request, feel free to **contact us**.

4. **HOW DO WE SHARE YOUR PERSONAL DATA AND WITH WHOM**

Alcoa will be able to share your personal data with third parties under the following circumstances:

0. **Service providers and business partners**. We will allow our service providers and business partners that perform certain services and other business operations for us to access to your personal data. [For example, We may partner with other companies to process secure payments, fulfill orders, optimize our services, send newsletters and marketing emails, support email and messaging services and analyze information.]. Before any access is granted to such third parties, We enter into a written agreement which requires them to refrain from making any further unauthorized disclosures of the personal data, to use the personal data only for the purposes of providing the specific services and according to the instructions received from Alcoa, to only retain the personal data as required to fulfill such purposes of protect our interests, and to have in place adequate and appropriate security measures.

1. **Alcoa Group companies**. Alcoa works closely with other businesses and companies that fall under the Alcoa group family. We will share certain information about you (e.g. your buying and browsing history on our website)] with other Alcoa Group companies for [marketing purposes and internal reporting].

2. **Law enforcement agency, court, regulator, government authority or other third party with compelling authority**. We will be able to share your personal data with these parties where we believe this is necessary to comply with a legal or regulatory obligation, or otherwise to protect our rights or the rights of any third party.

3. **Asset purchasers**. We will share your personal data with any third party that purchases, or to which We transfer, all or substantially all of our assets and business. Should such a sale or transfer occur, We will use reasonable efforts to ensure that the entity to which we transfer your personal data uses it in a manner that is consistent with this Privacy Policy.

Because We operate as part of a global business, the recipients referred to above can be located outside the jurisdiction in which you are located (or in which we provide the services), including third countries outside the European Union ("EU") that are not regarded as providing an adequate level of protection of the personal data. Please refer to the "International Data Transfer" section below for more information.

5. **HOW DO WE PROTECT YOUR PERSONAL DATA**

We implement technical and organizational measures to ensure a level of security appropriate to the risk to the personal data we process. These measures are aimed at ensuring the on-going integrity and confidentiality of personal data. We evaluate these measures on a regular basis to ensure the security of the processing.

6. **FOR HOW LONG DO WE STORE YOUR PERSONAL DATA**

We will keep your personal data for the length of time set out in our records retention policy.

7. **INTERNATIONAL DATA TRANSFERS**

Your personal data will be transferred to, stored, and processed in a country that is not regarded as ensuring an adequate level of protection for personal data under European Union law.

We have put in place appropriate safeguards (such as contractual commitments) in accordance with applicable legal requirements to ensure that your data is adequately protected, on the basis of the relevant sets of standard contractual clauses approved by the European Commission. For more information on the appropriate safeguards in place, please contact us at the details below.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at **http://www.jamsadr.com/international-mediation-rules**.

8. **CONTACT US**

Alcoa is the data controller with respect to the personal data We collect and process.

If you have questions or concerns regarding the way in which your personal data has been used, please **contact us**.

Our Data Protection Officer can be contacted at: **AlcoaDPO@alcoa.com**.

We are committed to working with you to obtain a fair resolution of any complaint or concern about privacy. If, however, you believe that We have not been able to assist with your complaint or concern, you have the right to make a complaint to the data protection authority of the applicable country where you reside using their website.

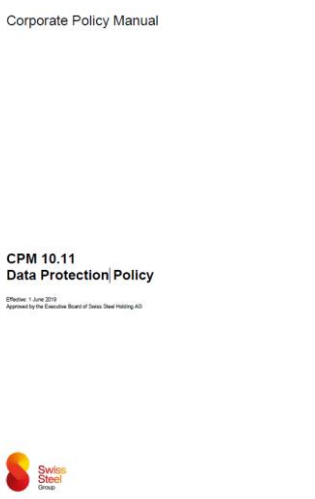
9. **CHANGES TO THIS PRIVACY POLICY**

You are entitled to request a copy of this Privacy Policy from us using the contact details set out above. This Privacy Policy will be subject to changes, as deemed necessary from time to time.

If We change this Privacy Policy, We will notify you of the changes. Where changes to the Privacy Policy will have a fundamental impact on the nature of the processing or otherwise have a substantial impact on you, We will give you sufficient advance notice so that you have the opportunity to exercise your rights (e.g. among other, to object to the processing). Moreover, and to the extent that Alcoa relies on consent for the performance of any of its processing activities, We will make sure to request your consent where the aforementioned changes may have a substantial impact on the relevant processing before these changes are made effective.

THIS ONLINE PRIVACY NOTICE TAKES EFFECT ON MAY 25, 2018

5.10 Annex 10 UGITECH's GDPR Policies



Corporate Policy Manual

CPM 10.11
Data Protection Policy

Effective: 1 June 2019
Approved by the Executive Board of Swiss Steel Holding AG

Swiss Steel Group

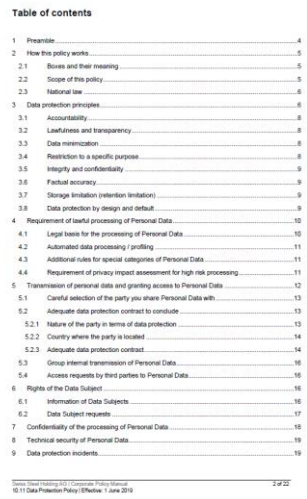
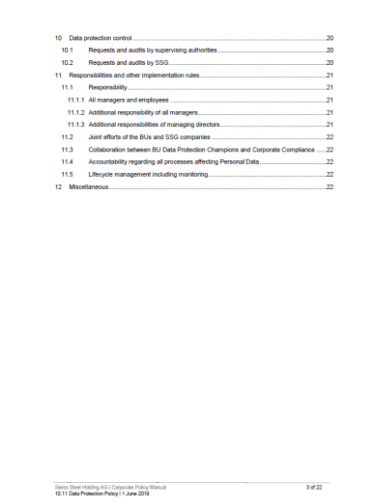
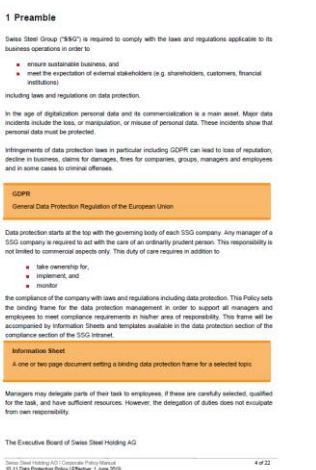


Table of contents





1 Preamble

Swiss Steel Group ("SSG") is required to comply with the laws and regulations applicable to its business operations in order to

- ensure sustainable business, and
- meet the expectation of external stakeholders (e.g. shareholders, customers, financial institutions)

including laws and regulations on data protection.

In the age of digitalization personal data and its commercialization is a main asset. Major data incidents include the loss, or manipulation, or misuse of personal data. These incidents show that personal data must be protected.

Infringements of data protection laws in particular including GDPR can lead to loss of reputation, decline in business, claims for damages, fines for companies, groups, managers and employees and in some cases to criminal offenses.

GDPR
General Data Protection Regulation of the European Union

Data protection starts at the top with the governing body of each SSG company. Any manager of a SSG company is required to act with the care of an ordinarily prudent person. This responsibility is not limited to commercial aspects only. This duty of care requires in addition to

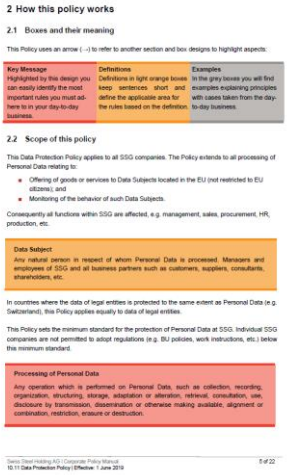
- take ownership for,
- implement, and
- monitor

the compliance of the company with laws and regulations including data protection. This Policy sets the binding frame for the data protection management in order to support all managers and employees to meet compliance requirements in his/her area of responsibility. This frame will be accompanied by Information Sheets and templates available in the data protection section of the compliance section of the SSG Intranet.

Information Sheet
A one or two page document setting a binding data protection frame for a selected topic

Managers may delegate parts of their task to employees, if these are carefully selected, qualified for the task, and have sufficient resources. However, the delegation of duties does not exculpate from own responsibility.

The Executive Board of Swiss Steel Holding AG



2 How this policy works

2.1 Boxes and their meaning

This Policy uses an arrow (→) to refer to another section and box designs to highlight aspects:

Key Message	Definitions	Examples
Highlighted by this design you can easily identify the most important rules you must adhere to in your day-to-day business.	Definitions in light orange boxes keep sentences short and define the applicable area for the rules based on the definition.	In the grey boxes you will find examples explaining principles with cases taken from the day-to-day business.

2.2 Scope of this policy

This Data Protection Policy applies to all SSG companies. The Policy extends to all processing of Personal Data relating to:

- Offering of goods or services to Data Subjects located in the EU (not restricted to EU citizens); and
- Monitoring of the behavior of such Data Subjects.

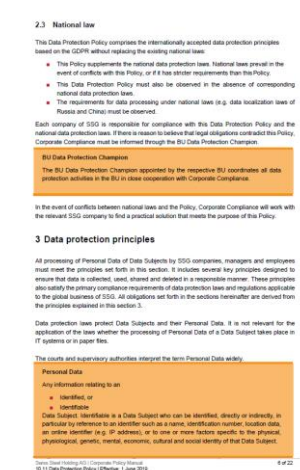
Consequently all functions within SSG are affected, e.g. management, sales, procurement, HR, production, etc.

Data Subject
Any natural person in respect of whom Personal Data is processed. Managers and employees of SSG and all business partners such as customers, suppliers, consultants, shareholders, etc.

In countries where the data of legal entities is protected to the same extent as Personal Data (e.g. Switzerland), this Policy applies equally to data of legal entities.

This Policy sets the minimum standard for the protection of Personal Data at SSG. Individual SSG companies are not permitted to adopt regulations (e.g. BU policies, work instructions, etc.) below this minimum standard.

Processing of Personal Data
Any operation which is performed on Personal Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.



2.3 National law

This Data Protection Policy comprises the internationally accepted data protection principles based on the GDPR without replacing the existing national laws.

- This Policy supplements the national data protection laws. National laws prevail in the event of conflicts with this Policy, or if it has stricter requirements than this Policy.
- This Data Protection Policy must also be observed in the absence of corresponding national data protection laws.
- The requirements for data processing under national laws (e.g. data localization laws of Russia and China) must be observed.

Each company of SSG is responsible for compliance with this Data Protection Policy and the national data protection laws. If there is reason to believe that legal obligations contradict this Policy, Corporate Compliance must be informed through the BU Data Protection Champion.

BU Data Protection Champion
The BU Data Protection Champion appointed by the respective BU coordinates all data protection activities in the BU in close cooperation with Corporate Compliance.

In the event of conflicts between national laws and the Policy, Corporate Compliance will work with the relevant SSG company to find a practical solution that meets the purpose of this Policy.

3 Data protection principles

All processing of Personal Data of Data Subjects by SSG companies, managers and employees must meet the principles set forth in this section. It includes several key principles designed to ensure that data is collected, used, shared and deleted in a responsible manner. These principles also satisfy the primary compliance requirements of data protection laws and regulations applicable to the global business of SSG. All obligations set forth in the sections hereinafter are derived from the principles explained in this section 3.

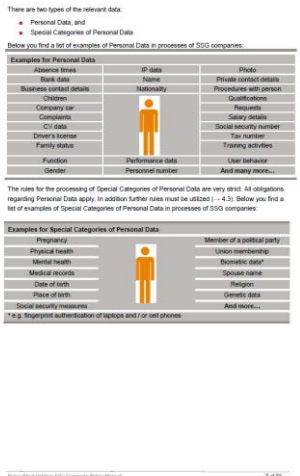
Data protection laws protect Data Subjects and their Personal Data. It is not relevant for the application of the laws whether the processing of Personal Data of a Data Subject takes place in IT systems or in paper files.

The courts and supervisory authorities interpret the term Personal Data widely.

Personal Data
Any information relating to an

- identified, or
- identifiable

Data Subject. Identifiable is a Data Subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier (e.g. IP address), or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural and social identity of that Data Subject.



There are two types of the relevant data:

- Personal Data, and
- Special Categories of Personal Data

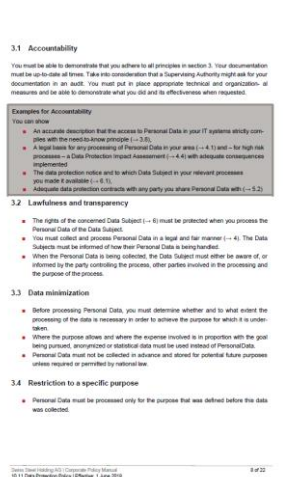
Below you find a list of examples of Personal Data in processes of SSG companies:

Examples for Personal Data		
Absence times	IP data	Photo
Bank data	Name	Private contact details
Business contact details	Nationality	Procedures with person
Children		Qualifications
Company car		Requests
Complaints		Salary details
CV/ data		Social security number
Driver's license		Tax number
Family status		Training activities
Function	Performance data	User behavior
Gender	Personnel number	And many more...

The rules for the processing of Special Categories of Personal Data are very strict. All obligations regarding Personal Data apply. In addition further rules must be utilized (→ 4.3). Below you find a list of examples of Special Categories of Personal Data in processes of SSG companies:

Examples for Special Categories of Personal Data		
Pregnancy		Member of a political party
Physical health		Union membership
Mental health		Biometric data*
Medical records		Spouse name
Date of birth		Religion
Place of birth		Genetic data
Social security measures		And more...

* e.g. fingerprint authentication of laptops and / or cell phones



3.1 Accountability

You must be able to demonstrate that you adhere to all principles in section 3. Your documentation must be up-to-date all times. Take into consideration that a Supervising Authority might ask for your documentation in an audit. You must put in place appropriate technical and organization- al measures and be able to demonstrate what you did and its effectiveness when requested.

Examples for Accountability
You can show

- An accurate description that the access to Personal Data in your IT systems strictly com- plies with the need-to-know principle (→ 3.6),
- A legal basis for any processing of Personal Data in your area (→ 4.1) and – for high risk processes – a Data Protection Impact Assessment (→ 4.4) with adequate consequences implemented
- The data protection notice and to which Data Subject in your relevant processes you made it available (→ 6.1),
- Adequate data protection contracts with any party you share Personal Data with (→ 5.2)

3.2 Lawfulness and transparency

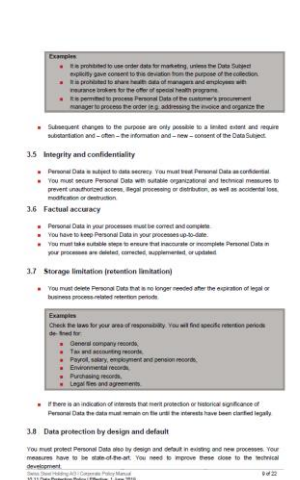
- The rights of the concerned Data Subject (→ 6) must be protected when you process the Personal Data of the Data Subject.
- You must collect and process Personal Data in a legal and fair manner (→ 4). The Data Subjects must be informed of how their Personal Data is being handled.
- When the Personal Data is being collected, the Data Subject must either be aware of, or informed by the party controlling the process, other parties involved in the processing and the purpose of the process.

3.3 Data minimization

- Before processing Personal Data, you must determine whether and to what extent the processing of the data is necessary in order to achieve the purpose for which it is under- taken.
- Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used instead of Personal Data.
- Personal Data must not be collected in advance and stored for potential future purposes unless required or permitted by national law.

3.4 Restriction to a specific purpose

- Personal Data must be processed only for the purpose that was defined before this data was collected.



Examples

- It is prohibited to use order data for marketing, unless the Data Subject explicitly gave consent to this deviation from the purpose of the collection.
- It is prohibited to share health data of managers and employees with insurance brokers for the offer of special health programs.
- It is permitted to process Personal Data of the customer's procurement manager to process the order (e.g. addressing the invoice and organize the

- Subsequent changes to the purpose are only possible to a limited extent and require substantiation and – often – the information and – new – consent of the Data Subject.

3.5 Integrity and confidentiality

- Personal Data is subject to data secrecy. You must treat Personal Data as confidential
- You must secure Personal Data with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

3.6 Factual accuracy

- Personal Data in your processes must be correct and complete.
- You have to keep Personal Data in your processes up-to-date.
- You must take suitable steps to ensure that inaccurate or incomplete Personal Data in your processes are deleted, corrected, supplemented, or updated.

3.7 Storage limitation (retention limitation)

- You must delete Personal Data that is no longer needed after the expiration of legal or business process-related retention periods.

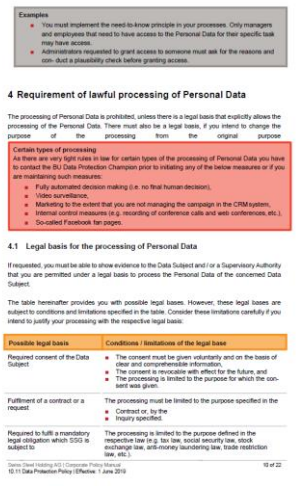
Examples
Check the laws for your area of responsibility. You will find specific retention periods de- fined for:

- General company records,
- Tax and accounting records,
- Payroll, salary, employment and pension records,
- Environmental records,
- Purchasing records,
- Legal files and agreements.

- If there is an indication of interests that merit protection or historical significance of Personal Data the data must remain on file until the interests have been clarified legally.

3.8 Data protection by design and default

You must protect Personal Data also by design and default in existing and new processes. Your measures have to be state-of-the-art. You need to improve these close to the technical development.



Examples
- You must implement the need-to-know principle in your processes. Only managers and employees that need to have access to the Personal Data for their specific task may have access.
- Administrators requested to grant access to someone must ask for the reasons and con- duct a plausibility check before granting access.

4 Requirement of lawful processing of Personal Data

The processing of Personal Data is prohibited, unless there is a legal basis that explicitly allows the processing of the Personal Data. There must also be a legal basis, if you intend to change the purpose of the processing from the original purpose

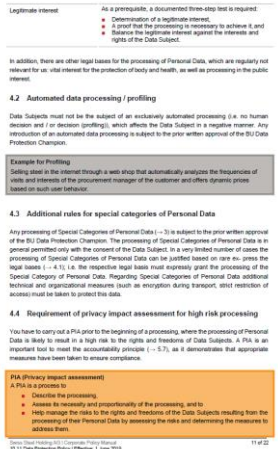
Certain types of processing
As there are very tight rules in law for certain types of the processing of Personal Data you have to contact the BU Data Protection Champion prior to initiating any of the below measures or if you are maintaining such measures:
- Fully automated decision making (i.e. no final human decision),
- Video surveillance,
- Marketing to the extent that you are not managing the campaign in the CRM system,
- Internal control measures (e.g. recording of conference calls and web conferences, etc.),
- So-called Facebook fan pages.

4.1 Legal basis for the processing of Personal Data

If requested, you must be able to show evidence to the Data Subject and / or a Supervisory Authority that you are permitted under a legal basis to process the Personal Data of the concerned Data Subject.

The table hereinafter provides you with possible legal bases. However, these legal bases are subject to conditions and limitations specified in the table. Consider these limitations carefully if you intend to justify your processing with the respective legal basis:

Possible legal basis	Conditions / limitations of the legal base
Required consent of the Data Subject	▪ The consent must be given voluntarily and on the basis of clear and comprehensible information. ▪ The consent is revocable with effect for the future, and ▪ The processing is limited to the purpose for which the consent was given.
Fulfilment of a contract or a request	The processing must be limited to the purpose specified in the ▪ Contract or, by the ▪ Inquiry specified.
Required to fulfill a mandatory legal obligation which SSG is subject to	The processing is limited to the purpose defined in the respective law (e.g. tax law, social security law, stock exchange law, anti-money laundering law, trade restriction law, etc.).



Legitimate interest	As a prerequisite, a documented three-step test is required: ▪ Determination of a legitimate interest, ▪ A proof that the processing is necessary to achieve it, and ▪ Balance the legitimate interest against the interests and rights of the Data Subject.

In addition, there are other legal bases for the processing of Personal Data, which are regularly not relevant for us: vital interest for the protection of body and health, as well as processing in the public interest.

4.2 Automated data processing / profiling

Data Subjects must not be the subject of an exclusively automated processing (i.e. no human decision and / or decision (profiling)), which affects the Data Subject in a negative manner. Any introduction of an automated data processing is subject to the prior written approval of the BU Data Protection Champion.

Example for Profiling
Selling steel in the internet through a web shop that automatically analyzes the frequencies of visits and interests of the procurement manager of the customer and offers dynamic prices based on such user behavior.

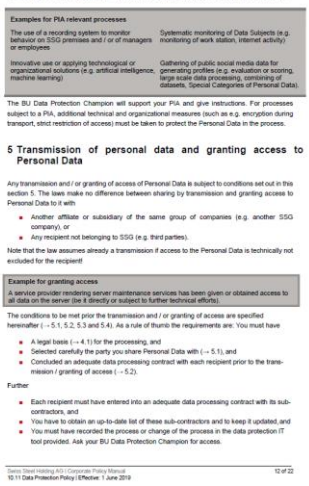
4.3 Additional rules for special categories of Personal Data

Any processing of Special Categories of Personal Data (→ 3) is subject to the prior written approval of the BU Data Protection Champion. The processing of Special Categories of Personal Data is in general permitted only with the consent of the Data Subject. In a very limited number of cases the processing of Special Categories of Personal Data can be justified based on rare ex- press the legal bases (→ 4.1), i.e. the respective legal basis must expressly grant the processing of the Special Category of Personal Data. Regarding Special Categories of Personal Data additional technical and organizational measures (such as encryption during transport, strict restriction of access) must be taken to protect this data.

4.4 Requirement of privacy impact assessment for high risk processing

You have to carry out a PIA prior to the beginning of a processing, where the processing of Personal Data is likely to result in a high risk to the rights and freedoms of Data Subjects. A PIA is an important tool to meet the accountability principle (→ 5.7), as it demonstrates that appropriate measures have been taken to ensure compliance.

PIA (Privacy impact assessment)
A PIA is a process to
- Describe the processing,
- Assess its necessity and proportionality of the processing, and to
- Help manage the risks to the rights and freedoms of the Data Subjects resulting from the processing of their Personal Data by assessing the risks and determining the measures to address them.



Contact the BU Data Protection Champion in case of high risk processes such as stated below:

Examples for PIA relevant processes	
The use of a recording system to monitor behavior on SSG premises and / or of managers or employees.	Systematic monitoring of Data Subjects (e.g. monitoring of work station, internet activity)
Innovative use or applying technological or organizational solutions (e.g. artificial intelligence, machine learning)	Gathering of public social media data for generating profiles (e.g. evaluation or scoring, large scale data processing, combining of datasets, Special Categories of Personal Data).

The BU Data Protection Champion will support your PIA and give instructions. For processes subject to a PIA, additional technical and organizational measures (such as e.g. encryption during transport, strict restriction of access) must be taken to protect the Personal Data in the process.

5 Transmission of personal data and granting access to Personal Data

Any transmission and / or granting of access of Personal Data is subject to conditions set out in this section 5. The laws make no difference between sharing by transmission and granting access to Personal Data to it with

- Another affiliate or subsidiary of the same group of companies (e.g. another SSG company), or
- Any recipient not belonging to SSG (e.g. third parties).

Note that the law assumes already a transmission if access to the Personal Data is technically not excluded for the recipient!

Example for granting access
A service provider rendering server maintenance services has been given or obtained access to all data on the server (be it directly or subject to further technical efforts).

The conditions to be met prior the transmission and / or granting of access are specified hereinafter (→ 5.1, 5.2, 5.3 and 5.4). As a rule of thumb the requirements are: You must have

- A legal basis (→ 4.1) for the processing, and
- Selected carefully the party you share Personal Data with (→ 5.1), and
- Concluded an adequate data processing contract with each recipient prior to the transmission / granting of access (→ 5.2).

Further

- Each recipient must have entered into an adequate data processing contract with its sub-contractors, and
- You have to obtain an up-to-date list of these sub-contractors and to keep it updated, and
- You must have recorded the process or change of the process in the data protection IT tool provided. Ask your BU Data Protection Champion for access.

5.1 Careful selection of the party you share Personal Data with

Ensuring an adequate level of data protection starts with the careful selection of the party you intend to share Personal Data with. Accordingly it is important to include in a request for quotation the data protection requirements. You need to choose this party based on

- The professional competence in the processing of Personal Data,
- State-of-the-art technical and organizational measures regarding all systems used for the processing,
- Experience in the market, and
- Other aspects evidencing reliability, e.g. data protection documentation, willingness to cooperate, responsiveness.

You remain responsible
You remain responsible for the Personal Data which you transmit or to which you grant access. In some cases you share this responsibility with the party you involve in the processing.

5.2 Adequate data protection contract to conclude

The contract you have to enter into with the party you intend to share Personal Data with (→ 5.2.3) depends on

- The nature of this party in terms of data protection (→ 5.2.1), and
- Where this party is located (→ 5.2.2)

5.2.1 Nature of the party in terms of data protection

The data protection law differentiates between two types of parties processing Personal Data: Controllers and Processors.

Controller	Processor
Controller is any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal	Processor is any natural person or company, public authority, agency or other body which processes personal data on behalf of the SSG company. The Controller – not the Processor – exclusively decides on the means and purpose

Examples for Controllers	Examples for Processors
▪ Your SSG company regarding the Personal Data of its main- agents and employees ▪ A travel agency your SSG company retains ▪ A credit card company your SSG company involves (e.g. using its Corporate Card or Company Card) ▪ Business relationships where often the both parties are Controllers: – Reporting to other group companies – Data access of an SSG company to the HR system of another SSG company (e.g. for performance-evaluation) – Group companies operate common systems (e.g. intranet, CRM). – Cross-company R&D platforms within the group as well as with customers or suppliers	▪ Cloud Providers, ▪ Service providers for implementation support, user support services, invoicing, system maintenance.

5.2.2 Country where the party is located

The law differentiates between countries with an adequate level of data protection and others. If the country, where the party you intend to share Personal Data with has an adequate level of data protection, it is easier to share Personal Data with.

List of Countries having Data Protection Adequacy
EU: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and – as long as so-called "BREXIT" is open – the UK (contact the BU Data Protection Champion upon BREXIT for instructions).
EEA: Iceland, Liechtenstein and Norway
Other: Switzerland, Israel, Japan, Canada, Argentina, Uruguay, New Zealand (in future upon further notice: South Korea)

Is the country of the party you intend to share Personal Data with not in the List of Countries having Data Protection Adequacy (e.g. the USA), you have to ensure sufficient guarantees by concluding an adequate data protection contract (→ 5.2.3) or proof other sufficient guarantees (e.g. binding corporate rules, approved certification mechanism).

5.2.3 Adequate data protection contract

Note: this section assumes that your SSG company acts as Controller (→ 5.2.1) in relation to the Personal Data you intend to share with the other party. Contact your BU Data Protection Champion if you have doubts, that your SSG company acts as Controller.

If the other party is a Processor while your SSG company is a Controller, you need to conclude a Controller-to-Processor contract depending on the location of the Processor:

Controller-to-Processor Contracts		
Location of Processor:	Country having Data Protection Adequacy (→ 5.2.1)	Other country
Adequate data protection contract:	Data Processing Agreement ("DPA")	Standard Contractual Clauses for Controller-to-Processor Processing ("SCC-P")

If the your SSG company and the other party are a Controller each in terms of the definition above (→ 5.2.3), you need to conclude a Controller contract depending on the location of the other party:

Controller Contracts		
Location of Controller	Country having Data Protection Adequacy (→ 5.2.1)	Other country
Adequate data protection contract:	Please contact Corporate Compliance if the commercial contract with the Controller does not cover data protection	Standard Contractual Clauses for Controller-to-Processor Processing ("SCC-C")

The SSG templates for the

- Controller-to-Processor Contracts (DPA and SCC-P), and the
- Controller Contract: SCC-C

are available in the data protection section of the compliance section of the SSG intranet.

5.3 Group internal transmission of Personal Data

Before you share Personal Data with any other SSG company – be it another affiliate, a BU holding company or SSG Holding AG – you have to check whether your SSG company has

- Entered into the SSG Intragroup Data Processing Agreement ("I-DPA"), and
- Whether the relevant process has been integrated into the I-DPA.

The first I-DPAs have been concluded for the HR software Talentsoft. Further I-DPAs will follow. Contact your BU Data Protection Champion for the relevant status information.

5.4 Access requests by third parties to Personal Data

If a manager or employee receives a request of someone else – be it another SSG company or an external party – to access Personal Data (e.g. about customers or employees), granting such access is permitted only

- Where the manager or employee intending to grant this access is able to prove a justified interest for this sharing, and
- A legal basis obliges (e.g. request by a tax authority) or allows (e.g. fulfillment of a contract, consent to sharing by Data Subject) to share the information, and
- The identity of the party requesting the access can be determined without any doubt.

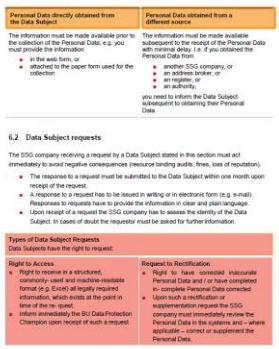
6 Rights of the Data Subject

Every Data Subject – independent of age, domicile or nationality – has the rights explained in this section 6.

6.1 Information of Data Subjects

SSG companies have to inform the Data Subject about the intended processing of the Personal Data of the Data Subject. This information can be issued by way of printed or electronic data protection notes within the framework of the collection procedure (e.g. internet and intranet of SSG company, recruiting portal of HR system, etc.). A template which has to be customized by you for the process oriented information is available in the data protection section of the compliance section of the SSG intranet.

When this information must be made available to the Data Subject depends on where the Personal Data to be processed is obtained from:



Personal Data directly obtained from the Data Subject	Personal Data obtained from a different source
The information must be made available prior to the collection of the Personal Data; e.g. you must provide the information ▪ in the web form, or ▪ attached to the paper form used for the collection	The information must be made available subsequent to the receipt of the Personal Data with minimal delay; i.e. if you obtained the Personal Data from ▪ another SSG company, or ▪ an address broker, or ▪ an register, or ▪ an authority, you need to inform the Data Subject subsequent to obtaining their Personal Data.

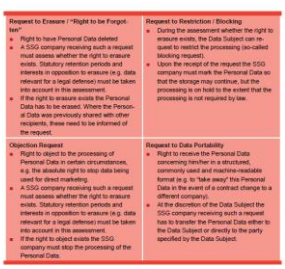
6.2 Data Subject requests

The SSG company receiving a request by a Data Subject stated in this section must act immediately to avoid negative consequences (resource binding audits, fines, loss of reputation).

- The response to a request must be submitted to the Data Subject within one month upon receipt of the request.
- A response to a request has to be issued in writing or in electronic form (e.g. e-mail). Responses to requests have to provide the information in clear and plain language.
- Upon receipt of a request the SSG company has to assess the identity of the Data Subject. In cases of doubt the requestor must be asked for further information.

Types of Data Subject Requests
Data Subjects have the right to request:

Right to Access	Request to Rectification
▪ Right to receive in a structured, commonly- used and machine-readable format (e.g. Excel) all legally required information, which exists at the point in time of the re- quest, ▪ Inform immediately the BU Data Protection Champion upon receipt of such a request	▪ Right to have corrected inaccurate Personal Data and / or have completed in- complete Personal Data corrected ▪ Upon such a rectification or supplementation request the SSG company must immediately review the Personal Data in the systems and – where applicable – correct or supplement the Personal Data.



Request to Erasure / "Right to be Forgotten"	Request to Restriction / Blocking
▪ Right to have Personal Data deleted ▪ A SSG company receiving such a request must assess whether the right to erasure exists. Statutory retention periods and interests in opposition to erasure (e.g. data relevant for a legal defense) must be taken into account in this assessment. ▪ If the right to erasure exists the Personal Data has to be erased. Where the Personal Data was previously shared with other recipients, these need to be informed of the request.	▪ During the assessment whether the right to erasure exists, the Data Subject can request to restrict the processing (so-called blocking request). ▪ Upon the receipt of the request the SSG company must mark the Personal Data so, that the storage may continue, but the processing is on hold to the extent that the processing is not required by law.
Objection Request	**Request to Data Portability**
▪ Right to object to the processing of Personal Data in certain circumstances, e.g. the absolute right to stop data being used for direct marketing. ▪ A SSG company receiving such a request must assess whether the right to erasure exists. Statutory retention periods and interests in opposition to erasure (e.g. data relevant for a legal defense) must be taken into account in this assessment. ▪ If the right to object exists the SSG company must stop the processing of the Personal Data.	▪ Right to receive the Personal Data concerning him/her in a structured, commonly used and machine-readable format (e.g. to "take away" this Personal Data in the event of a contract change to a different company), ▪ At the discretion of the Data Subject the SSG company receiving such a request has to transfer the Personal Data either to the Data Subject or directly to the party specified by the Data Subject.

7 Confidentiality of the processing of Personal Data

The processing of Personal Data is subject to confidentiality. Prior to taking up their activities all managers and employees must be instructed by their manager to keep Personal Data confidential. Managers and employees are in particular prohibited to

- Use Personal Data for private purposes,
- Disclose it to unauthorized persons, or
- Make it available in any other way to unauthorized recipients.

In order to support by design the confidentiality you have to implement the "need-to-know" principle. Managers and employees must have access to Personal Data only as the access is appropriate for the scope of their specific task. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities in all processes.

8 Technical security of Personal Data

SSG companies have to implement appropriate technical and organizational measures ("TOM") in order to protect the Personal Data. This applies to Personal Data processed electronically or in paper form, even though the TOMs may vary. The TOMs form part of the security concept at SSG and also protect our business secrets. TOMs must continuously being adapted to technical developments and organizational changes. Efforts and protection should be in an adequate balance.

Examples for TOMs

- Process description of denial of admittance to data-processing equipment/systems for unauthorized persons
- Ability to ensure protecting Personal Data from unauthorized reading, copying, changing or deletion, and ensuring traceability of data transfer operations by using Pseudonymization and/or encryption
- Ability to ensure the ongoing confidentiality, integrity, availability and resilience of its information technology systems
- Ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident
- Process implemented for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

The competent IT department is responsible for the TOMs in IT systems of the SSG company as well as the assessment of the TOMs of Processors retained by the SSG company (→ 5.2.1).

The management of an SSG company is responsible for the TOMs regarding Personal Data in paper form (e.g. "clean desk policy", entrance control).

9 Data protection incidents

Act immediately
In case of a possible data protection incident, the SSG company affected must act immediately as the relevant supervisory authorities must be informed within 72 hours. Further, it might be necessary to inform the Data Subjects affected by the incident.

Data protection incident
A breach or potential breach of protection of Personal Data leading to the

- Unauthorized or accidental disclosure of, or access to, Personal Data,
- An unauthorized or accidental alteration of Personal Data, or loss of access to, or destruction of Personal Data, or
- The temporary loss of availability of Personal Data, as a lack of access to such data can have significant impact on the rights and freedoms of Data Subjects.

If you have identified or have the suspicion of the existence of a data protection incident within SSG or any of its subcontractors, you have immediately to inform

- The BU Data Protection Champion of your SSG company. The relevant contact data is available on the Data Protection Incident web page in the data protection section of the compliance section of the SSG intranet.
- Corporate Compliance, and
- Corporate IT.

Examples

- Personal data of customers was accidentally visible on the website,
- Personal Data has been stolen by a targeted attack,
- An e-mail with Personal Data has accidentally been sent to an incorrect recipient.
- A loss of electronic devices (e.g. notebook, cell phone, USB stick, etc.)

In parallel you have to complete on the same day the **Data Protection Incident Form** available on the Data Protection Incident web page in the SSG intranet. Upon completion you have to submit the form to the BU Data Protection Champion, Corporate Compliance, and Corporate IT and follow their instructions, e.g. informing the Data Protection Officer.

Data Protection Incident Form
A form you must complete in case of a data protection incident or a respective suspicion. Based on the completed form, the BU Data Protection Champion makes an analysis of the incident, compiles further in collaboration with you information if necessary and assesses whether:

- Communication to the affected Data Subject is required and / or
- Notification to the competent data protection supervisory authority must be filed.

10 Data protection control

10.1 Requests and audits by supervising authorities

Supervising authorities may at any time request information about the processing of Personal Data at any SSG company and / or may audit any SSG company. Any SSG manager or employee receiving such a request or getting contacted at the beginning of any audit activity must immediately contact

- The BU Data Protection Champion, and
- Corporate Compliance.

10.2 Requests and audits by SSG

Compliance with this Data Protection Policy and the applicable data protection laws is checked frequently with data protection audits and other controls.

11 Responsibilities and other implementation rules

11.1 Responsibility

11.1.1 All managers and employees

Whatever your role at SSG is, you must commit to Data Protection Policy in the work you do every day in its scope (→ 2.2). The Data Protection Policy sets the boundaries which all at SSG must operate without exception every day. Make yourself familiar and understand the risks in your role and how to manage these. Seek advice from your BU Data Protection Champion when things are not clear. Make sure that anyone you exchange Personal Data with or you grant access to Personal Data to is aware that we at SSG are all bound by our Data Protection Policy, and expect business partners to act accordingly.

11.1.2 Additional responsibility of all managers

We depend on our managers to promote our ethical standards and act as role models for their teams regarding this Data Protection Policy. We expect managers to show leadership in following Data Protection Policy and facilitate and maintain a culture of commitment to it. We expect managers to implement this Data Protection Policy in their area of responsibility, e.g.

- Ensure a permanently up-to-date recording of all processes affecting Personal Data,
- Conduct on each process a gap-analysis,
- Implement gap-closing measures,
- Track in their area of responsibility the implementation of this Policy as requested by the BU Data Protection Champion, and
- Report the implementation status of the tasks the BU Data Protection requested to perform to the BU Data Protection Champion.

Our managers have to understand the risks associated with Personal Data in their area according to this Policy. The managers have to develop and implement procedures to mitigate these risks. Our managers also have to be alert to any violation of the Data Protection Policy, and encourage their team members to speak up if they know or suspect a violation.

11.1.3 Additional responsibilities of managing directors

Our Managing Directors bear the legal responsibility for the implementation of data protection laws and this Policy in their SSG company. Managing Directors in addition have to maintain a constantly up-to-date register for their SSG company listing

- If applicable (e.g. Germany): the Data Protection Officer appointed for the SSG company
- One Data Protection Coordinator for the SSG company supporting the BU Data Protection Champion by supporting, advising and controlling the implementation of this Data Protection Policy and related obligations in the respective SSG company
- Process Owners for each process affecting Personal Data, responsible for the implementation of this Data Protection Policy and related obligations in the respective process. As such the Process Owner must be familiar with the purpose of the process and any process step.
- System Owners for each IT system, responsible for the implementation of technical data protection (→ 8) and IT security measures defined by Corporate of BU IT in the respective IT system.

Where reasonable SSG managers or employees of other SSG companies might be appointed as Data Protection Coordinator and / or System Owner in agreement with the Managing Director of the other SSG company. The details of the roles and responsibilities are defined in the data protection section of the forthcoming Data Protection Management System Description.

11.2 Joint efforts of the BUs and SSG companies

The managers, in particular those in the same SSG Company, BU and / or at the same SSG location, should jointly implement the Data Protection Policy where possible and efficient. Accordingly managers affected should exchange frequently on their Data Protection Management System and an efficient implementation strategy. The BU Data Protection Champions support the managers by coordination and advice.

11.3 Collaboration between BU Data Protection Champions and Corporate Compliance

The BU Data Protection Champions act as support function for the managers and employees of their BU and give advice to these in terms of the Data Protection Policy and limited to the area of responsibility defined in the Data Protection Policy, and the particular function of the respective member of the compliance organization. Corporate Compliance acts as support function of the BU Data Protection Champions and gives advice to these.

11.4 Accountability regarding all processes affecting Personal Data

It is required that the measures required by this Data Protection Policy will be appropriately recorded in accordance with the local retention laws.

11.5 Lifecycle management including monitoring

The manager or employee dealing with processes affecting Personal Data is accountable (→ 3.1; i.e. responsible for the entire documentation) for the Lifecycle Management.

Lifecycle Management

- The documentation of the processes affecting Personal Data have to be up-to-date, e.g. the process description in the data protection IT tool (currently DPM of PwC) must be updated with any process change (e.g. change of the purpose of the processing, the application or the Processor involved).
- The same applies to other documentation (e.g. contracts with suppliers and group companies, description of access concept and system changes).

12 Miscellaneous

The effective date of the Data Protection Policy is June 1st, 2019. The Data Protection Policy is effective for an unlimited period of time and will be reviewed and amended from time to time (e.g. when the EU e-Privacy Directive comes into force around the year 2020).


HEATERNAL