

AGREEMENT

regarding Processor's Processing of Personal Data on behalf of the Controller

(hereinafter referred to as "DPA")

between

xxx-AG

Address

CH-xxxxxxxxx

hereinafter referred to as “**Controller**”

and

SPIE ICS AG

Sonnenplatz 6

CH-6020 Emmenbrücke

hereinafter referred to as “**Processor**”

hereinafter both together referred to as “**the Parties**”

**Contents**

[1 Introduction 3](#_Toc106284608)

[2 Scope of this DPA 3](#_Toc106284609)

[3 Controller's Rights, Obligations and Warranty 3](#_Toc106284610)

[4 Obligations of the Processor 4](#_Toc106284611)

[5 Subprocessing 6](#_Toc106284612)

[6 Term and Termination 7](#_Toc106284613)

[7 Payment 7](#_Toc106284614)

[8 Governing Law 7](#_Toc106284615)

[9 Jurisdiction 8](#_Toc106284616)

[10 Miscellaneous 8](#_Toc106284617)

[11 Definitions 8](#_Toc106284618)

[12 Signatures 10](#_Toc106284619)

# Introduction

* 1. The Controller wishes to mandate or has mandated the Processor with the provision of services for the benefit of the Controller and the Processor wishes to accept or has accepted such mandate, based on an ongoing collaboration between the Parties and/or an agreement, whether in writing or not, defining the services and the terms of service provision (collectively **"Agreement"**).The services, which the Processor provides for the benefit of the Controller, shall be referred to as **Services**.
  2. In rendering the Services, the Processor may Process Relevant Data on behalf of the Controller.
  3. For such situations, the Applicable Data Protection Law may set forth the obligation for the Controller and the Processor to enter into an agreement governing such Processing.
  4. Should the Processor be Processing Relevant Data according to the Applicable Data Protection Law and should that Applicable Data Protection Law set forth the obligation to enter into an agreement governing such Processing, then this DPA contains the terms and conditions applicable to the Processing of such Relevant Data with the aim to ensure that both Parties comply with the Applicable Data Protection Law.
  5. Based thereon, the Parties agree to this DPA with the rights and obligations set forth herein.

# Scope of this DPA

* 1. The Processor has been or will be mandated with the provision of Services for the benefit of the Controller. The provision of Services includes the Processing of Relevant Data on behalf of the Controller. This DPA sets forth in the following the Parties' obligations and acknowledgements with view to Processor's processing of Relevant Data on behalf of the Controller.
  2. The details of the Processing operation provided by the Processor to the Controller as a commissioned data processor (e.g., the subject-matter of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects) are specified in Annex 1 to this DPA.

# Controller's Rights, Obligations and Warranty

* 1. The Controller warrants to be the Controller of the Relevant Data as defined herein.
  2. The Controller remains the responsible Controller for the Processing of the Relevant Data.
  3. The Controller is entitled and obliged to instruct the Processor in connection with the Processing of the Relevant Data, generally or in the individual case. Instructions may also relate to the correction, deletion, blocking of the Relevant Data. Upon request, the Controller shall specify its order, instructions and comments more precisely.
  4. The Controller agrees and warrants to comply with its protection, security and other obligations with respect to Relevant Data prescribed by Applicable Data Protection Law for data controllers by: (a) establishing and maintaining a procedure for the exercise of the rights of the individuals whose Personal Data are processed on behalf of the Controller; (b) Processing only Relevant Data that has been lawfully and validly collected and ensuring that such data will be relevant and proportionate to the respective uses; and (c) ensuring compliance with the provisions of this DPA by its personnel or by any third-party accessing or using Relevant Data on its behalf.
  5. The Controller agrees to hold the Processor, its Affiliates, and its respective agents, officers, directors, shareholders, partners, employees and licensees, and each of their successors and permitted assigns (collectively, the "Indemnified Parties") harmless and defend them ("defend" only at the Indemnified Parties' option) from and against any and all claims and demands (collectively, "Claims"), brought by a third party based upon or arising in any manner, directly or indirectly, out of or in connection with Controller's breach of its aforementioned warranty. The Controller shall pay all damages and reimburse the Indemnified Parties for the incurred costs, including without limitation, reasonable legal fees arising out of and in connection with any such Claims. The Indemnified Parties must notify the Controller promptly in writing of any claim for indemnification hereunder, and provide, at the Controller's expense (to the extent of out-of-pocket expenses only), all reasonably necessary assistance, information and authority to allow the Controller to control the defense and settlement of such Claim should the Indemnified Parties have chosen this option. Notwithstanding the foregoing, the Controller shall not enter into any settlement, other than with respect to the payment of monies, without the Indemnified Parties' prior written consent.

# Obligations of the Processor

The Processor shall:

* 1. Comply with and act only on instructions from and on behalf of the Controller regarding the Processing of Relevant Data. Such obligation also applies to the transfer of Relevant Data to a third country.
  2. Within a reasonable period of time, notify the Controller, where the Processor in its opinion believes that an instruction of the Controller would obviously result in a violation of Applicable Data Protection Law and request Controller to withdraw, amend or confirm the relevant instruction. Pending the decision on the withdrawal, amendment or confirmation of the relevant instruction, the Processor shall be entitled to suspend the implementation of the relevant instruction. It remains understood that the overall responsibility as to compliance with the Applicable Data Protection Law remains with the Controller.
  3. Not Process Relevant Data for any other purposes other than to provide the services to the Controller.
  4. Ensure that persons authorized by the Processor to Process the Relevant Data on behalf of the Controller are suitably informed, trained and instructed in respect of Applicable Data Protection Law and have committed themselves in writing to confidentiality or are under an appropriate statutory obligation of confidentiality. The Processor will undertake commercially reasonable efforts that such authorized persons observe any Applicable Data Protection Law beyond their respective employment periods in respect of the Relevant Data.
  5. Implement the Technical and Organizational Measures which will meet the requirements of Applicable Data Protection Law before Processing the Relevant Data and ensure to provide sufficient guarantees to the Controller on such Technical and Organizational Measures. For this purpose, the Processor has in place an information security management system that is maintained in alignment with international standards and best practices. The Parties understand and agree that the obligation to implement such Technical and Organizational Measures is strictly limited to the systems, processes and infrastructures, which are under the direct control of the Processor. The Processor shall not be held liable for systems, processes and infrastructures or any consequences arising out of the non-compliance of any systems, processes and infrastructures, which are not under the direct control of the Processor.
  6. Assist the Controller by appropriate Technical and Organizational Measures, insofar as this is possible, for the fulfillment of Controller's obligation to respond to requests for exercising Data Subjects' rights concerning information, access, rectification and erasure, restriction of Processing, notification, data portability, objection and automated decision-making.
  7. Take actions requested or instructed by the Controller in order to comply with Data Subject's rights under Applicable Data Protection Law. In particular, Processor must provide the information on action taken on such request without undue delay, respectively in a timely manner.
  8. Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and in Art. 28 GDPR or in Art. 10a FDPA, as the case may be.
  9. Allow for and contribute to audits, limited in scope to the assessment of compliance with this DPA. Expenses incurred on Processor's side in connection with such audit shall be reimbursed by the Controller. Any third-party costs in connection with such audit shall be borne by the Party requesting it. Such audit may only be undertaken maximum once a year and only by an independent third-party auditor with no conflict of interests.
  10. Notify the Controller without undue delay:
      1. about any legally binding request for disclosure of the Relevant Data by a law enforcement authority, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
      2. about any complaints and requests received directly from Data Subjects (e.g., regarding access, rectification, erasure, restriction of Processing, data portability, objection to Processing of data, automated decision-making) without responding to that request, unless it has been otherwise authorized to do so;
      3. after Processor becomes aware of a Personal Data Breach at Processor or its Subprocessors. In case of such Personal Data Breach, Service Provider will assist Controller with investigating the Personal Data Breach and Controller's obligation under Applicable Data Protection Law to inform the Data Subjects and the Supervisory Authorities, as applicable, and to document the Personal Data Breach.
  11. Assist Controller with any data protection impact assessment and with prior consultation, if any, that relate to the Services provided by Processor to Controller and the Relevant Data Processed on behalf of Controller.

# Subprocessing

* 1. Controller authorizes the engagement of Processor's Affiliates as Subprocessors.
  2. Controller likewise authorizes the engagement of third parties as Subprocessors which are referred to in Processor’s offer, Service description, Agreement, referenced documentation or online locations, etc.
  3. Processor shall inform Controller about any intended changes concerning the addition or replacement of third-party Subprocessors, thereby giving Controller the opportunity to object to such changes within 90 days after which Controller shall be deemed to have accepted the new third-party Subprocessor.
  4. Any subcontract with a third party by which any Processing of Relevant Data is subcontracted must in compliance with the Applicable Data Protection Law.
  5. Processor must ensure contractually that with respect to the subcontracted portion of the Processing of Relevant Data the Subcontractor has obligations vis-a-vis the Processor corresponding to those of the Processor vis-a-vis the Controller, in particular that the Subprocessor provides sufficient guarantees to implement appropriate Technical and Organizational Measures in such a manner that the Processing will meet the requirements of Applicable Data Protection Law.
  6. Where a Subprocessor fails to fulfill its data protection obligations, Processor shall remain fully liable to Controller for the performance of the Subprocessor's obligations.
  7. In case any such Subprocessor is located outside Europe in a country that is not recognized by the Supervisory Authority as providing an adequate level of data protection, Processor will conclude with the relevant Subprocessor the relevant SCC.

# Term and Termination

* 1. The term of this DPA is identical with the term of the relevant Agreement or in the case of ongoing/subsequent business relationships under different agreements, identical with the longest term of such agreements.
  2. The Processor shall, at the choice of the Controller, delete or return all Relevant Data to the Controller after the end of the provision of Services, and delete any existing copies. The Processor may retain one copy of the Personal Data for evidence purposes and/or for the establishment, exercise or defence of legal claims and/or to comply with applicable laws and regulations.

# Payment

* 1. All amounts payable for the Services provided by the Processor as well as the payment terms are set forth in the Agreement. No further payment or any other consideration shall be due in connection with this DPA, except as expressly set out otherwise in this DPA.
  2. Expenses must be reimbursed to the Processor.

# Governing Law

* 1. The DPA shall be governed by and interpreted in accordance with the Swiss law, without giving effect to its rules of conflict of laws and regardless of the place of its physical execution or performance.

# Jurisdiction

* 1. Any disputes relating to this DPA shall be dealt with exclusively by the ordinary courts of Bern, without restricting any right of appeal. Notwithstanding the above, each of the Party shall, however, be authorized to seek interim orders and injunctive measures before any competent authority worldwide.

# Miscellaneous

* 1. Should one of the provisions of this DPA be or become invalid, the validity of the DPA as a whole shall not be affected. The invalid or void provision shall be replaced by such valid provision as the Parties would have agreed had they known of the invalidity at the time of concluding the DPA on order to achieve the same economic result.
  2. This DPA constitutes the entire understanding of the Parties with respect to the subject matter hereof and cancel and supersede any previous agreement, understanding negotiations or discussion, both written and oral, and whether explicit or implicit, between the Parties before the execution hereof.

# Definitions

* 1. **"Europe Data Protection Law(s)"** shall mean all data protection laws and regulations applicable to Europe, as well as their amendments or revisions and implementing ordinances, including (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii); (iv) Swiss Federal Data Protection Act of 19 June 1993 ("**FDPA**")**;** and (v) in respect of the United Kingdom ("**UK**")any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK having left the European Union;
  2. **"Europe"** shall mean, for the purposes of this DPA, the European Union, the European Economic Area and/or their member states, Switzerland and the UK.
  3. **“Applicable Data Protection Law”** shall mean the laws and regulations within the Europe Data Protection Laws that govern the duties of and apply to the specific Party and its Processing activity in question.
  4. **"Supervisory Authority"** shall mean an independent public authority which is established pursuant to Europe Data Protection Law, for example pursuant to Article 51 of the GDPR or, in relation to Switzerland, the Swiss Federal Commissioner for Data Protection and Information.
  5. **"Technical and Organizational Measures"** shall mean those measures aimed at protecting Personal Data against accidental destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.
  6. **"SCC"** shall mean the standard contractual clauses as approved by the European Commission or any Supervisory Authority in Europe (as applicable) for safeguarding transfers of Personal Data for Processing to recipients in countries not recognized as providing an adequate level of data protection by the competent authority as per Europe Data Protection Law.
  7. **"Affiliate(s)"** means any domestic or foreign company established at the date of signature hereto that is directly or indirectly controlled by the concerned Party or its parent company or in which the concerned Party or its parent company holds directly or indirectly at least 50% of its share capital.
  8. **“Relevant Data”** means Personal Data Processed by Processor on behalf of Controller based on the Agreement in connection with rendering the Services.
  9. **“Data Subject(s)”, “Personal Data”, “Controller”, “Processor”, “Subprocessor”, “Personal Data Breach”, “Process”, “Special Categories of Data”,** shall have the same meaning as in the GDPR.

# Signatures

The undersigned Parties agree with this DPA, dated as of Effective Date, and its terms.

The Parties agree that this DPA may be executed in hard copy by means of hand-written signatures or, alternatively, in soft copy by means of electronic signatures standards with legally binding effect as per the applicable laws.

**xxx-AG:**

Place and date:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature authorized signatory Signature authorized signatory

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name in block letters Name in block letters

**SPIE ICS AG:**

Place and date:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature authorized signatory Signature authorized signatory

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name in block letters Name in block letters

Annex 2: Technical and organizational Measures of the Processor

*The Processor shall list here an exhaustive list of measures to protect the data, and can also reference any information security or data protection certification or management system.*

1. Confidentiality

## Access

*Measures that are suitable for denying unauthorized persons access to data processing systems with which personal data is processed or used. Among other things, automatic access control systems, the use of chip cards and transponders, access control by gatekeepers and alarm systems can be used as access control measures for building and room security. Servers, telecommunications systems, network technology and similar systems must be protected in lockable server cabinets. In addition, it makes sense to support access control with organizational measures (e.g. service instructions that provide for the locking of the offices in case of absence).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical measures** | | **Organizational measures** | |
|  | Alarm |  | Key regulation / list |
|  | Automatic access control system |  | Reception / Reception / Doorman |
|  | Biometric access locks |  | Visitor's book / protocol of visitors |
|  | Chip cards / transponder systems |  | Employee / visitor badges |
|  | Manual locking system |  | Visitors accompanied by staff |
|  | Security locks |  | Care in the selection of security guards |
|  | Locking system with code lock |  | Care in the selection of cleaning services |
|  | Protection of the building shafts |  |  |
|  | Doors with knob on the outside |  |  |
|  | Bell system with camera |  |  |
|  | Video surveillance of the entrances |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Further/other measures:

## Physical access control

*Measures that are suitable to prevent data processing systems (computers) from being used by unauthorized persons.*

*Access control refers to the prevention of the unauthorized use of equipment. Possibilities are, for example, boot password, user ID with password for operating systems and software products used, screensavers with password, the use of chip cards for login as well as the use of call-back procedures. In addition, organizational measures may also be necessary, for example, to prevent unauthorized access (e.g. specifications for the installation of screens, issuing guidance for users on how to choose a "good" password).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical measures** | | **Organizational measures** | |
|  | Login with username + password |  | Managing User Permissions |
|  | Login with username + password + second factor |  | Creating User Profiles |
|  | Login with biometric data |  | Central password assignment |
|  | Anti-Virus Software Server |  | Strong Password Policy |
|  | Anti-virus software clients |  | "Delete/Destroy" policy |
|  | Anti-virus software mobile devices |  | Clean Desk Policy |
|  | Firewall |  | General Data Protection and/or Security Policy |
|  | Intrusion Detection Systems |  | Mobile Device Policy |
|  | Mobile Device Management |  | Manual Desktop Lock Guide |
|  | Use of VPN for remote access |  |  |
|  | Encryption of data carriers |  |  |
|  | Encryption Smartphones |  |  |
|  | Housing interlock |  |  |
|  | BIOS protection (separate password) |  |  |
|  | Blocking external interfaces (USB) |  |  |
|  | Automatic desktop lock |  |  |
|  | Encryption of notebooks / tablets |  |  |
|  |  |  |  |

Further/other measures:

## Access control

*Measures to ensure that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage. Access control can be ensured, among other things, by suitable authorization concepts that enable differentiated control of access to data. It is important to differentiate between the content of the data and the possible access functions to the data. Furthermore, suitable control mechanisms and responsibilities must be defined in order to document the assignment and revocation of authorizations and to keep them up to date (e.g. in the event of recruitment, change of job, termination of the employment relationship). Particular attention must always be paid to the role and possibilities of administrators.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical measures** | | **Organizational measures** | |
|  | File shredder (min. level 3 / DIN 3, cross cut) |  | Use of authorization concepts |
|  | External shredder (DIN32757) |  | Minimum number of administrators |
|  | Physical deletion of disks |  | Privacy Vault |
|  | Logging of access to applications, specifically when entering, modifying and deleting data |  | Administration of user rights by administrators |
|  |  |  |  |
|  |  |  |  |

Further/other measures:

## Separation control

*Measures to ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical measures** | | **Organizational measures** | |
|  | Separation of production and test environment |  | Control via authorization concept |
|  | Physical separation (systems / databases / data carriers) |  | Determination of database rights |
|  | Multi-tenancy of relevant applications |  | Datasets are tagged with purpose attributes |
|  |  |  |  |
|  |  |  |  |

Further/other measures:

## Anonymization / Pseudonymization / Encryption

*The processing of personal data is carried out in such a way that the data can no longer be assigned to a specific data subject without the use of additional information, provided that this additional information is stored separately and is subject to appropriate technical and organizational measures.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical measures** | | **Organizational measures** | |
|  | In the case of pseudonymization:  Separation of assignment data and storage in a separate and secure system (possibly encrypted) |  | Internal instruction to anonymize / pseudonymize personal data as far as possible in the event of disclosure or even after expiry of the statutory deletion period |
|  | The data is anonymized and cannot be assigned to a single person. |  |  |
|  | Encryption |  |  |
|  |  |  |  |

Further/other measures:

1. Integrity

## Passing on control

*measures to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or transport or storage on data carriers, and that it is possible to verify and establish to which entities personal data are intended to be transferred by data transmission facilities. To ensure confidentiality in electronic data transmission, e.g. encryption techniques and virtual private networks can be used. Measures for data carrier transport or data transfer are transport containers with locking devices and regulations for data protection-compliant destruction of data carriers.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical measures** | | **Organizational measures** | |
|  | Encryption of data |  | Documentation of the data recipients as well as the duration of the planned transfer or the deletion periods |
|  | Use of VPN |  | Overview of regular call-off and  Submission operations |
|  | Logging of accesses and retrievals |  | Disclosure in anonymized or pseudonymized form |
|  | Safe transport containers |  | Care in the selection of transport personnel and vehicles |
|  | Deployment via encrypted connections such as sftp, https |  | Personal handover with protocol |
|  | Use of signature procedures |  | Choosing a reliable transporter |
|  |  |  |  |
|  |  |  |  |

Further/other measures:

## Input control

*Measures to ensure that it can be subsequently checked and determined whether and by whom personal data has been entered, changed or removed from data processing systems. Input control is achieved through logging, which can take place at different levels (e.g. operating system, network, firewall, database, application). It must also be clarified which data is logged, who has access to logs, by whom and on what occasion/time they are checked, how long storage is required and when the logs are deleted.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical measures** | | **Organizational measures** | |
|  | Technical logging of the entry, modification and deletion of data |  | Overview of which programs can be used to enter, change or delete which data |
|  | Manual or automated control of logs |  | Traceability of input, modification and deletion of data by individual user names (not user groups) |
|  | Logging of administrator activities |  | Assignment of rights to enter, change and delete data on the basis of an authorization concept |
|  | Protection of log data against loss or alteration |  | Retention of forms from which data has been transferred to automated processing |
|  |  |  | Clear responsibilities for deletions |
|  |  |  |  |

Further/other measures:

# Availability and resilience

## Availability check

*Measures to ensure that personal data is protected against accidental destruction or loss. This involves topics such as an uninterruptible power supply, air conditioning, fire protection, data backups, secure storage of data carriers, virus protection, raid systems, disk mirroring, etc.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical measures** | | **Organizational measures** | |
|  | Fire and smoke detection systems |  | Backup & Recovery concept (formulated) |
|  | Fire extinguisher server room |  | Control of the backup process |
|  | Server room monitoring temperature  and humidity |  | Regular tests for data recovery and logging of results |
|  | Air-conditioned server room |  | Storage of the backup media on  a safe place outside the  Server room |
|  | UPS |  | No sanitary connections in the or  above the server room |
|  | Protective power strips server room |  | Existence of an emergency plan (e.g. BSI IT-Grundschutz 100-4) |
|  | Privacy vault (S60DIS, S120DIS,  other suitable standards with swelling seals, etc.) |  | Separate partitions for operating systems and data |
|  | RAID System / Disk Mirroring |  |  |
|  | Video surveillance server room |  |  |
|  | Alarm message in case of unauthorized access to server room |  |  |
|  |  |  |  |
|  |  |  |  |

Further/other measures:

# Periodic review, assessment and evaluation procedures

## Data Protection Management

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical measures** | | **Organizational measures** | |
|  | Software solutions for data protection  Management in action |  | Internal/external data protection officer  Name / Company / Contact Details |
|  | Central documentation of all procedures and regulations on data protection with access for employees as required / authorization (e.g. wiki, intranet ...) |  | Employees trained and committed to confidentiality/data secrecy |
|  | Security certification according to ISO 27001, BSI IT-Grundschutz or ISIS12 |  | Regular sensitization of employees At least once a year |
|  | Other documented security concept |  | Internal / External Information Security Officer Name / Company Contact |
|  | A review of the effectiveness of the technical protection measures is carried out at least annually |  | The Data Protection Impact Assessment (DPIA) will be carried out if necessary |
|  |  |  | The organization complies with the information obligations pursuant to Art. 13 and 14 GDPR |
|  |  |  | Formalized process for processing requests for information from data subjects is in place |
|  |  |  |  |

Further/other measures:

## Incident Response Management

*Assistance in responding to security breaches*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical measures** | | **Organizational measures** | |
|  | Use of firewall and regular updating |  | Documented process for detecting and reporting security incidents / data breaches (also with regard to reporting obligations to the supervisory authority) |
|  | Use of spam filters and regular updates |  | Documented procedure for dealing with security incidents |
|  | Use of virus scanner and regular updates |  | Involvement of DPOs and ISBs in security incidents and data breaches |
|  | Intrusion Detection System (IDS) |  | Documentation of security incidents and data breaches, e.g. via ticket system |
|  | Intrusion Prevention System (IPS) |  | Formal process and responsibilities for the follow-up of security incidents and data breaches |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Further/other measures:

## Privacy-friendly preferences

*Privacy by design / Privacy by default*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical measures** | | **Organizational measures** | |
|  | No more personal data is collected than is necessary for the respective purpose |  |  |
|  | Simple exercise of the right of withdrawal  of the person concerned by technical measures |  |  |
|  |  |  |  |
|  |  |  |  |

Further/other measures:

## Order control

*Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions. In addition to data processing on behalf of the customer, this also includes the performance of maintenance and system support work both on site and remotely. If the Processor uses service providers/Subprocessors in the sense of order processing, the following points must always be regulated with them.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical measures** | | **Organizational measures** | |
|  |  |  | Prior examination of the security measures taken by the Subprocessor and their documentation |
|  |  |  | Obligation of the Subprocessor’s employees to maintain data secrecy |
|  |  |  | Obligation to appoint a data protection officer by the  Subprocessor in the event of an obligation to appoint |
|  |  |  | Agreement on effective control rights vis-à-vis the Processor |
|  |  |  | Regulation on the use of additional Subprocessors |
|  |  |  | Ensuring the destruction of data after completion of the order |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Further/other measures:

**xxx-AG:**

Place and date:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature authorized signatory Signature authorized signatory

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name in block letters Name in block letters

# Annex 1 – Details of the processing

**The subject matter defined in the contract/customer agreement includes the following processing**

|  |
| --- |
|  |

*(Specify the subject of the contract/customer agreement or, description of the agreed and provided services.)*

**Nature and purpose of the processing**

|  |
| --- |
|  |

*(More detailed description, reference to contract/customer agreement if applicable).*

**Location of the processing**

|  |
| --- |
|  |

*(Where is the personal data processed and/or where can the personal data be accessed? If relevant, list reference to 'approved subcontractors').*

**Duration of the processing**

|  |
| --- |
|  |

*(How long is the data processed, during and after the end of the contract and how is the data deleted ).*

**Categories and type of personal data**

|  |
| --- |
|  |

*(Which personal data categories are processed, and what type of data)*

**Data transfers**

|  |
| --- |
|  |

*(To whom is data transferred and what protective measures have been taken. Description of the measures for transfer or access, and in to which countries, third country)*

**Controller: contact person for data protection or DPO**

|  |
| --- |
|  |

*(Name, Function, Phone number. E-Mail, Address)*

**SPIE: contact person for data protection**

|  |
| --- |
| Eduardo GERALDI  CISO  Freiburgstrasse 251  3018 Bern  Tel: + 41 58 301 19 05  E-Mail [dpo.ch@spie.com](mailto:dpo.ch@spie.com) |

**xxx-AG:**

Place and date:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature authorized signatory Signature authorized signatory

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name in block letters Name in block letters

**SPIE ICS AG:**

Place and date:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature authorized signatory Signature authorized signatory

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Eduardo GERALDI Name in block letters