

ACCORD concernant le traitement des données A Caractère personnel  
par le sous-traitant pour le compte du Responsable de traitement

(ci-après dénommée "**DPA**")

entre

xxx-AG

Adresse

CH-xxxxxxxxx

ci-après dénommé "**Responsable de traitement**".

et

SPIE ICS AG

Sonnenplatz 6

CH-6020 Emmenbrücke

ci-après dénommé "**Sous-traitant**".

ci-après dénommées ensemble les "**les Parties**" et individuellement la "**Partie**".

**Contenu**

[1 Introduction 3](#_Toc130905831)

[2 Champ d'application de ce DPA 3](#_Toc130905832)

[3 Droits, obligations et garantie du Responsable du traitement 3](#_Toc130905833)

[4 Obligations du Sous-traitant 4](#_Toc130905834)

[5 Sous-traitement 6](#_Toc130905835)

[6 Durée et résiliation 7](#_Toc130905836)

[7 Paiement 7](#_Toc130905837)

[8 Loi applicable 7](#_Toc130905838)

[9 Compétence 7](#_Toc130905839)

[10 Divers 7](#_Toc130905840)

[11 Définitions 7](#_Toc130905841)

[12 Signatures 8](#_Toc130905842)

# Introduction

* 1. Le Responsable du traitement souhaite mandater ou a mandaté le Sous-traitant pour la fourniture de services au profit du Responsable du traitement et le Sous-traitant souhaite accepter ou a accepté ce mandat, sur la base d'une collaboration continue entre les Parties et/ou d'un accord, écrit ou non, définissant les services et les conditions de fourniture des services (collectivement **" Accord "**). Les services, que le Sous-traitant fournit au profit du Responsable du traitement, sont désignés par le terme " **Services "**.
  2. Dans le cadre de la prestation de Services, le Sous-traitant peut traiter des Données pertinentes pour le compte du Responsable de traitement.
  3. Pour ces situations, la loi applicable en matière de protection des données peut prévoir l'obligation pour le Responsable de traitement et le Sous-traitant de conclure un accord régissant ce traitement.
  4. Si le Sous-traitant traite des Données pertinentes conformément à la Loi applicable sur la protection des données et si cette Loi applicable sur la protection des données prévoit l'obligation de conclure un accord régissant ce traitement, alors le présent DPA contient les termes et conditions applicables au traitement de ces Données pertinentes dans le but de garantir que les deux Parties respectent la Loi applicable sur la protection des données.
  5. Sur cette base, les parties conviennent du présent DPA avec les droits et obligations qui y sont énoncés.

# Champ d'application de ce DPA

* 1. Le Sous-traitant a été ou sera mandaté pour la fourniture de Services au profit du Responsable du traitement. La fourniture des Services comprend le traitement des Données pertinentes pour le compte du Responsable de traitement. Le présent DPA énonce ci-après les obligations et reconnaissances des Parties en ce qui concerne le traitement par le Sous-traitant des Données pertinentes pour le compte du Responsable de traitement.
  2. Les détails du traitement fournis par le Sous-traitant au Responsable du traitement en tant que sous-traitant de données mandaté (par exemple, l'objet du traitement, la nature et la finalité du traitement, le type de Données à caractère personnel et les catégories de Personnes concernées) sont précisés à l'annexe 1 du présent DPA.

# Droits, obligations et garantie du Responsable du traitement

* 1. Le Responsable du traitement garantit qu'il est le Responsable du traitement des données pertinentes telles que définies dans les présentes.
  2. Le Responsable du traitement reste le Responsable du traitement des données pertinentes.
  3. Le Responsable du traitement a le droit et l'obligation de donner des instructions au Responsable du traitement dans le cadre du traitement des Données pertinentes, de manière générale ou dans le cas individuel. Les instructions peuvent également porter sur la correction, l'effacement, le blocage des Données pertinentes. Sur demande, le Responsable du traitement spécifie plus précisément son ordre, ses instructions et ses commentaires.
  4. Le Responsable du traitement accepte de et garantit se conformer à ses obligations de protection, de sécurité et autres obligations relatives aux Données pertinentes prescrites par la Loi applicable sur la protection des données pour les Responsables du traitements de données en : (a) établissant et maintenant une procédure pour l'exercice des droits des individus dont les Données Personnelles sont traitées pour le compte du Responsable du traitement ; (b) traitant uniquement les Données pertinentes qui ont été légalement et valablement collectées et en s'assurant que ces données seront pertinentes et proportionnées aux utilisations respectives ; et (c) assurant le respect des dispositions du présent DPA par son personnel ou par tout tiers accédant ou utilisant les Données pertinentes pour son compte.
  5. Le Responsable du traitement accepte de dégager le Sous-traitant, ses sociétés affiliées et ses agents, dirigeants, administrateurs, actionnaires, partenaires, employés et titulaires de licence respectifs, ainsi que chacun de leurs successeurs et ayants droit autorisés (collectivement, les "Parties Indemnisées") et les défendre ("défendre" uniquement au choix des Parties Indemnisées) contre toutes les réclamations et demandes (collectivement, les "réclamations") présentées par un tiers et fondées ou découlant de quelque manière que ce soit, directement ou indirectement, de la violation par le Responsable du traitement de la garantie susmentionnée. Le Responsable du traitement doit payer tous les dommages-intérêts et rembourser aux Parties Indemnisées les frais encourus, y compris, mais sans s'y limiter, les frais juridiques raisonnables découlant de ces Réclamations et en rapport avec celles-ci. Les Parties Indemnisées doivent notifier rapidement par écrit au Responsable du traitement toute demande d'indemnisation au titre des présentes et fournir, aux frais du Responsable du traitement (dans la limite des seuls frais remboursables), toute l'assistance, les informations et l'autorité raisonnablement nécessaires pour permettre au Responsable du traitement de contrôler la défense et le règlement de ladite Réclamation si les Parties Indemnisées ont choisi cette option. Nonobstant ce qui précède, le Responsable du traitement ne doit pas conclure de règlement, autre que le paiement de sommes d'argent, sans le consentement écrit préalable des Parties Indemnisées.

# Obligations du Sous-traitant

Le Sous-traitant doit :

4.1. Se conformer et agir uniquement sur les instructions du Responsable du traitement et en son nom concernant le traitement des Données pertinentes. Cette obligation s'applique également au transfert des Données pertinentes vers un pays tiers.

4.2. Dans un délai raisonnable, notifier au Responsable du traitement, lorsque le Sous-traitant estime qu'une instruction du Responsable du traitement entraînerait manifestement une violation de la législation applicable en matière de protection des données et demander au Responsable du traitement de retirer, modifier ou confirmer l'instruction en question. Dans l'attente de la décision sur le retrait, la modification ou la confirmation de l'instruction concernée, le Sous-traitant est en droit de suspendre l'exécution de l'instruction concernée. Il reste entendu que la responsabilité globale du respect de la loi applicable à la protection des données incombe au Responsable du traitement.

4.3. Ne pas traiter les Données pertinentes à d'autres fins que celles de fournir les Services au Responsable du traitement.

4.4. S'assurer que les personnes autorisées par le Sous-traitant à traiter les Données pertinentes pour le compte du Responsable du traitement sont convenablement informées, formées et instruites en ce qui concerne le Droit applicable à la protection des données et se sont engagées par écrit à respecter la confidentialité ou sont soumises à une obligation légale de confidentialité appropriée. Le Sous-traitant s'efforcera, dans la mesure du raisonnable, de faire en sorte que ces personnes autorisées respectent toute Loi applicable à la protection des données au-delà de leurs périodes d'emploi respectives en ce qui concerne les Données pertinentes.

4.5. Mettre en œuvre les mesures techniques et organisationnelles qui répondront aux exigences de la loi applicable en matière de protection des données avant de traiter les données pertinentes et s'assurer de fournir des garanties suffisantes au Responsable du traitement sur ces mesures techniques et organisationnelles. À cette fin, le Sous-traitant a mis en place un système de gestion de la sécurité de l'information qui est maintenu en conformité avec les normes et les meilleures pratiques internationales. Les Parties comprennent et conviennent que l'obligation de mettre en œuvre ces Mesures Techniques et Organisationnelles est strictement limitée aux systèmes, processus et infrastructures, qui sont sous le contrôle direct du Sous-traitant. Le Sous-traitant ne peut être tenu responsable des systèmes, processus et infrastructures ou de toute conséquence découlant de la non-conformité de tout système, processus et infrastructure, qui ne sont pas sous le contrôle direct du Sous-traitant.

4.6. Assister le Responsable du traitement par des Mesures techniques et organisationnelles appropriées, dans la mesure où cela est possible, pour l'accomplissement de l'obligation du Responsable du traitement de répondre aux demandes d'exercice des droits des Personnes concernées concernant l'information, l'accès, la rectification et l'effacement, la limitation du traitement, la notification, la portabilité des données, l'opposition et la prise de décision automatisée.

4.7. Prendre les mesures demandées ou instruites par le Responsable du traitement afin de se conformer aux droits de la Personne concernée en vertu du droit applicable à la protection des données. En particulier, le Sous-traitant doit fournir les informations sur les mesures prises à la suite d'une telle demande sans retard excessif, respectivement en temps opportun.

4.8. Mettre à la disposition du Responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues par le présent DPA et par l'art. 28 GDPR ou à l'art. 10a de la LPFD, selon le cas.

4.9. Permettre et contribuer à des audits, dont la portée est limitée à l'évaluation du respect du présent DPA. Les frais engagés par le Sous-traitant dans le cadre de cet audit sont remboursés par le Responsable du traitement. Tous les frais de tiers liés à cet audit sont à la charge de la Partie qui le demande. Cet audit ne peut être entrepris qu'une fois par an au maximum et uniquement par un auditeur tiers indépendant et sans conflit d'intérêts.

4.10. Notifier le Responsable du traitement sans délai excessif :

* + 1. sur toute demande juridiquement contraignante de divulgation des Données pertinentes par une autorité chargée de l'application de la loi, sauf interdiction contraire, telle qu'une interdiction en vertu du droit pénal pour préserver la confidentialité d'une enquête policière ;
    2. sur les plaintes et les demandes reçues directement des Personnes concernées (par exemple, concernant l'accès, la rectification, l'effacement, la restriction du traitement, la portabilité des données, l'opposition au traitement des données, la prise de décision automatisée) sans répondre à cette demande, sauf s'il a été autrement autorisé à le faire ;
    3. après que le Sous-traitant a eu connaissance d'une violation de données à caractère personnel chez le Sous-traitant ou chez ses sous-traitants. Dans le cas d'une telle violation de données à caractère personnel, le Prestataire de services aidera le Responsable du traitement à enquêter sur la violation de données à caractère personnel et sur l'obligation du Responsable du traitement, en vertu de la loi applicable sur la protection des données, d'informer les Personnes concernées et les Autorités de contrôle, le cas échéant, et de documenter la violation de données à caractère personnel.
  1. Assister le Responsable du traitement dans toute évaluation d'impact sur la protection des données et dans toute consultation préalable, le cas échéant, qui se rapporte aux Services fournis par le Sous-traitant au Responsable du traitement et aux Données pertinentes traitées pour le compte du Responsable du traitement.

# Sous-traitement

* 1. Le Responsable du traitement autorise l'engagement des sociétés affiliées du Sous-traitant en tant que sous-traitants secondaires.
  2. Le Responsable du traitement autorise également l'engagement de tiers en tant que sous-traitants secondaires auxquels il est fait référence dans l'offre du Sous-traitant, la description du service, l'accord, la documentation référencée ou les sites en ligne, etc.
  3. Le Sous-traitant informe le Responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement de sous-traitants secondaires tiers, donnant ainsi au Responsable du traitement la possibilité de s'opposer à ces changements dans un délai de 90 jours, après quoi le Responsable du traitement est réputé avoir accepté le nouveau sous-traitant secondaire tiers.
  4. Tout contrat de sous-traitance avec un tiers par lequel un traitement des Données pertinentes est sous-traité doit être conforme à la Loi sur la protection des données applicable.
  5. Le Sous-traitant doit s'assurer contractuellement qu'en ce qui concerne la partie sous-sous-traitée du traitement des Données pertinentes, le sous-sous-traitant a des obligations vis-à-vis du Sous-traitant correspondant à celles du Sous-traitant vis-à-vis du Responsable du traitement, en particulier que le sous-sous-traitant fournit des garanties suffisantes pour mettre en œuvre des Mesures techniques et organisationnelles appropriées de telle sorte que le traitement réponde aux exigences du Droit applicable en matière de protection des données.
  6. Lorsqu'un sous-sous-traitant ne remplit pas ses obligations en matière de protection des données, le Sous-traitant reste entièrement responsable envers le Responsable du traitement de l'exécution des obligations du sous-sous-traitant.
  7. Dans le cas où un tel sous-sous-traitant est situé en dehors de l'Europe dans un pays qui n'est pas reconnu par l'autorité de contrôle comme offrant un niveau adéquat de protection des données, le Sous-traitant conclura avec le sous-sous-traitant concerné la CCT pertinente.

# Durée et résiliation

6.1 La durée du présent DPA est identique à celle de l'accord concerné ou, en cas de relations commerciales continues/successives dans le cadre de différents accords, identique à la durée la plus longue de ces accords.

6.2. Le Sous-traitant doit, au choix du Responsable du traitement, supprimer ou renvoyer toutes les Données pertinentes au Responsable du traitement après la fin de la fourniture des Services, et supprimer toute copie existante. Le Sous-traitant peut conserver une copie des Données à caractère personnel à des fins de preuve et/ou pour l'établissement, l'exercice ou la défense de réclamations légales et/ou pour se conformer aux lois et réglementations applicables.

# Paiement

7.1. Tous les montants payables pour les services fournis par le Sous-traitant ainsi que les modalités de paiement sont énoncés dans le contrat. Aucun autre paiement ni aucune autre contrepartie n'est dû en relation avec le présent DPA, sauf disposition contraire expresse dans le présent DPA.

7.2. Les dépenses doivent être remboursées au Sous-traitant.

# Loi applicable

* 1. Le DPA est régi et interprété conformément au droit suisse, sans donner effet à ses règles de conflit de lois et indépendamment du lieu de son exécution ou de sa réalisation physique.

# Compétence

* 1. Tout litige relatif au présent DPA sera traité exclusivement par les tribunaux ordinaires de Lausanne /Genève [*biffer ce qui ne convient pas*], sans restriction des voies de recours. Nonobstant ce qui précède, chacune des parties est toutefois autorisée à demander des ordonnances provisoires et des mesures d'injonction auprès de toute autorité compétente dans le monde entier.

# Divers

* 1. Si l'une des dispositions du présent DPA est ou devient invalide, la validité de l'ensemble du DPA n'est pas affectée. La disposition invalide ou nulle sera remplacée par la disposition valide dont les parties auraient convenu si elles avaient eu connaissance de l'invalidité au moment de la conclusion de l'AAP, afin d'obtenir le même résultat économique.
  2. Le présent DPA constitue l'intégralité de l'accord des parties concernant l'objet des présentes et annule et remplace tout accord, entente, négociation ou discussion antérieurs, écrits ou oraux, explicites ou implicites, entre les parties avant la signature des présentes.

# Définitions

11.1 **" Loi(s) européenne(s) sur la protection des données "** désigne toutes les lois et tous les règlements sur la protection des données applicables en Europe, ainsi que leurs modifications ou révisions et leurs ordonnances d'application, notamment (i) le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (" **GDPR** ") ; (ii) la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ; (iii) les mises en œuvre nationales applicables de (i) et (ii) ; (iv) la loi fédérale suisse sur la protection des données du 25 septembre 2020 (" **LPD** ") **;** et (v) en ce qui concerne le Royaume-Uni (" **RU** "), toute législation nationale applicable qui remplace ou convertit en droit interne le GDPR ou toute autre loi relative aux données et à la vie privée en conséquence du fait que le RU a quitté l'Union européenne ;

11.2. **" Europe "** désigne, aux fins du présent DPA, l'Union européenne, l'Espace économique européen et/ou leurs États membres, la Suisse et le Royaume-Uni.

11.3 **" Loi applicable sur la protection des données "** désigne les lois et règlements au sein des lois européennes sur la protection des données qui régissent les devoirs de la Partie spécifique et de son activité de traitement en question et s'appliquent à celle-ci.

11.4 **" Autorité de contrôle "** désigne une autorité publique indépendante qui est établie conformément à la loi européenne sur la protection des données, par exemple en vertu de l'article 51 du RGPD ou, en ce qui concerne la Suisse, le Préposé fédéral à la protection des données et à l'information.

11.5. **" Mesures techniques et organisationnelles "** désigne les mesures visant à protéger les Données à caractère personnel contre la destruction accidentelle ou la perte accidentelle, l'altération, la divulgation ou l'accès non autorisé, notamment lorsque le traitement implique la transmission de données sur un réseau, et contre toute autre forme illicite de traitement.

11.6 **" CCT "** désigne les clauses contractuelles types telles qu'approuvées par la Commission européenne ou toute autorité de contrôle en Europe (selon le cas) pour la sauvegarde des transferts de Données à caractère personnel en vue de leur traitement vers des destinataires situés dans des pays non reconnus comme assurant un niveau adéquat de protection des données par l'autorité compétente conformément à la loi européenne sur la protection des données.

11.7. **" Affilié(s) "** : toute société nationale ou étrangère établie à la date de signature des présentes, contrôlée directement ou indirectement par la partie concernée ou sa société mère ou dans laquelle la partie concernée ou sa société mère détient directement ou indirectement au moins 50 % de son capital social.

11.8. **" Données pertinentes "** désigne les Données à caractère personnel traitées par le Sous-traitant pour le compte du Responsable du traitement sur la base de l'Accord dans le cadre de la prestation des Services.

* 1. **" Personne(s) concernée(s) ", " Données à caractère personnel ", " Responsable du traitement ", " Sous-traitant ", " Sous-sous-traitant ", " Violation de données à caractère personnel ", " Processus ", " Catégories spéciales de données ",** ont la même signification que dans le GDPR.

# Signatures

Les Parties soussignées acceptent le présent DPA, daté de la date d'entrée en vigueur, et ses conditions.

Les Parties conviennent que le présent DPA peut être exécuté sur support papier au moyen de signatures manuscrites ou, à défaut, sur support électronique au moyen de normes de signatures électroniques ayant un effet juridiquement contraignant conformément aux lois applicables.

**xxx-AG :**

Lieu et date :

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

Signature du signataire autorisé Signature du signataire autorisé

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

Nom en lettres majuscules Nom en lettres majuscules

**SPIE ICS AG :**

Lieu et date :

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

Signature du signataire autorisé Signature du signataire autorisé

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

Nom en lettres majuscules Nom en lettres majuscules

# 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

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