

VEREINBARUNG

über die bearbeitung personenbezogener Daten durch den Auftragsbearbeiter im Auftrag des Verantwortlichen

(im Folgenden als "**DPA**" bezeichnet)

zwischen

xxx-AG

Adresse

CH-xxxxxxxxx

im Folgenden als"**Verantwortlicher**" bezeichnet

und

SPIE ICS AG

Sonnenplatz 6

CH-6020 Emmenbrücke

im Folgenden als "**Auftragsbearbeiter**" bezeichnet

im Folgenden beide zusammen als "**die Parteien**" bezeichnet

**Inhalt**

[1 Einführung 3](#_Toc106284608)

[2 Geltungsbereich dieses DPA 3](#_Toc106284609)

[3 Rechte, Pflichten und Gewährleistung des Verantwortlichen 3](#_Toc106284610)

[4 Pflichten des Auftragsbearbeiters 4](#_Toc106284611)

[5 Weiterverarbeitung 6](#_Toc106284612)

[6 Laufzeit und Beendigung 7](#_Toc106284613)

[7 Zahlung 7](#_Toc106284614)

[8 Geltendes Recht 7](#_Toc106284615)

[9 Zuständigkeitsbereich 8](#_Toc106284616)

[10 Sonstiges 8](#_Toc106284617)

[11 Definitionen 8](#_Toc106284618)

[12 Unterschriften 10](#_Toc106284619)

# Einführung

* 1. Der Verantwortliche möchte den Auftragsbearbeiter mit der Erbringung von Dienstleistungen zugunsten des Verantwortlichen beauftragen oder hat ihn damit beauftragt, und der Auftragsbearbeiter möchte diesen Auftrag annehmen oder hat ihn angenommen, und zwar auf der Grundlage einer laufenden Zusammenarbeit zwischen den Parteien und/oder einer schriftlichen oder nicht schriftlichen Vereinbarung, in der die Dienstleistungen und die Bedingungen für die Erbringung der Dienstleistungen festgelegt sind (zusammenfassend **"Vereinbarung"**). Die Dienstleistungen, die der Auftragsbearbeiter zugunsten des Verantwortlichen erbringt, werden als **Dienstleistungen** bezeichnet.
  2. Bei der Erbringung der Dienstleistungen kann der Auftragsbearbeiter relevante Daten im Auftrag des Verantwortlichen bearbeiten.
  3. In solchen Fällen kann das geltende Datenschutzrecht die Verpflichtung des Verantwortlichen und des Auftragsbearbeiters vorsehen, eine Vereinbarung über die Bearbeitung zu schliessen.
  4. Sollte der Auftragsbearbeiter relevante Daten gemäss dem geltenden Datenschutzrecht bearbeiten und sollte dieses geltende Datenschutzrecht die Verpflichtung zum Abschluss einer Vereinbarung über eine solche Bearbeitung vorsehen, dann enthält dieses DPA die für die Bearbeitung dieser relevanten Daten geltenden Bedingungen mit dem Ziel, sicherzustellen, dass beide Parteien das geltende Datenschutzrecht einhalten.
  5. Auf dieser Grundlage vereinbaren die Parteien dieses DPA mit den hierin festgelegten Rechten und Pflichten.

# Geltungsbereich dieses DPA

* 1. Der Auftragsbearbeiter wurde oder wird mit der Erbringung von Dienstleistungen zugunsten des Verantwortlichen beauftragt. Die Erbringung von Dienstleistungen umfasst die Bearbeitung relevanter Daten im Auftrag des Verantwortlichen. Dieses DPA legt im Folgenden die Verpflichtungen und Anerkennungen der Parteien im Hinblick auf die Bearbeitung relevanter Daten durch den Auftragsbearbeiter im Auftrag des Verantwortlichen fest.
  2. Die Einzelheiten der Bearbeitung, die der Auftragsbearbeiter dem Verantwortlichen als Auftragsdatenbearbeiter zur Verfügung stellt (z. B. der Gegenstand der Bearbeitung, die Art und der Zweck der Bearbeitung, die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen), sind in Anhang 1 zu diesem DPA aufgeführt.

# Rechte, Pflichten und Gewährleistungen des Verantwortlichen

* 1. Der Verantwortliche garantiert, dass er der für die relevanten Daten Verantwortliche ist, wie hier definiert.
  2. Der Verantwortliche bleibt für die Bearbeitung der relevanten Daten verantwortlich.
  3. Der Verantwortliche ist berechtigt und verpflichtet, dem Auftragsbearbeiter im Zusammenhang mit der Bearbeitung der relevanten Daten allgemein oder im Einzelfall Weisungen zu erteilen. Die Weisungen können sich auch auf die Berichtigung, Löschung oder Sperrung der betroffenen Daten beziehen. Auf Wunsch präzisiert der Verantwortliche seine Aufträge, Weisungen und Bemerkungen.
  4. Der Verantwortliche erklärt sich damit einverstanden und gewährleistet, dass er seinen Schutz-, Sicherheits- und sonstigen Verpflichtungen in Bezug auf die relevanten Daten, die das geltende Datenschutzrecht für die Verantwortlichen vorschreibt, nachkommt, indem er: (a) ein Verfahren zur Ausübung der Rechte der Personen, deren personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet werden, einrichtet und aufrechterhält; (b) nur rechtmässig und gültig erhobene relevante Daten bearbeitet und sicherstellt, dass diese Daten für die jeweiligen Verwendungszwecke relevant und verhältnismässig sind; und (c) die Einhaltung der Bestimmungen dieses DPA durch seine Mitarbeiter oder durch Dritte, die in seinem Auftrag auf relevante Daten zugreifen oder diese verwenden, sicherstellt.
  5. Der Verantwortliche erklärt sich damit einverstanden, den Auftragsbearbeiter, seine verbundenen Unternehmen und seine jeweiligen Vertreter, leitenden Angestellten, Direktoren, Aktionäre, Partner, Mitarbeiter und Lizenznehmer sowie alle ihre Nachfolger und zulässigen Rechtsnachfolger (zusammen, die "**freigestellten Parteien**") schadlos zu halten und zu verteidigen ("verteidigen" nur nach Wahl der freigestellten Parteien) von und gegen alle Ansprüche und Forderungen (zusammenfassend "**Ansprüche**"), die von einem Dritten aufgrund oder in irgendeiner Weise, direkt oder indirekt, aus oder im Zusammenhang mit der Verletzung der vorgenannten Garantie durch den Verantwortlichen erhoben werden. Die verantwortliche Stelle trägt alle Schäden und erstattet den freigestellten Parteien die entstandenen Kosten, einschließlich, aber nicht beschränkt auf, angemessene Anwaltskosten, die sich aus und im Zusammenhang mit solchen Ansprüchen ergeben. Die freigestellten Parteien müssen die verantwortliche Stelle unverzüglich schriftlich über jeden Anspruch auf Entschädigung im Rahmen dieser Vereinbarung unterrichten und auf Kosten der verantwortlichen Stelle (nur in Höhe der Auslagen) alle vernünftigerweise erforderliche Unterstützung, Informationen und Befugnisse bereitstellen, damit die verantwortliche Stelle die Verteidigung und Beilegung eines solchen Anspruchs kontrollieren kann, falls die freigestellten Parteien diese Option gewählt haben. Ungeachtet des Vorstehenden schließt der Verantwortliche ohne vorherige schriftliche Zustimmung der freigestellten Parteien keinen Vergleich, der nicht die Zahlung von Geldern zum Gegenstand hat.

# Pflichten des Auftragsbearbeiters

Der Auftragsbearbeiter ist verpflichtet:

* 1. Die Anweisungen des Verantwortlichen zu befolgen und nur in seinem Namen zu handeln, wenn es um die Bearbeitung relevanter Daten geht. Diese Verpflichtung gilt auch für die Übermittlung relevanter Daten in ein Drittland.
  2. Innerhalb einer angemessenen Frist den Verantwortlichen zu benachrichtigen, wenn der Auftragsbearbeiter der Ansicht ist, dass eine Anweisung des Verantwortlichen offensichtlich zu einem Verstoss gegen das geltende Datenschutzrecht führen würde, und den Verantwortlichen aufzufordern, die betreffende Anweisung zurückzuziehen, zu ändern oder zu bestätigen. Bis zur Entscheidung über den Widerruf, die Änderung oder die Bestätigung der betreffenden Weisung ist der Auftragsbearbeiter berechtigt, die Durchführung der betreffenden Weisung auszusetzen. Es versteht sich von selbst, dass die Gesamtverantwortung für die Einhaltung der geltenden Datenschutzgesetze bei dem Verantwortlichen verbleibt.
  3. Die relevanten Daten nicht für andere Zwecke als die Erbringung der Dienstleistungen für den Verantwortlichen zu bearbeiten.
  4. Sicherzustellen, dass die vom Auftragsbearbeiter zur Bearbeitung der relevanten Daten im Auftrag des Verantwortlichen befugten Personen angemessen über die geltenden Datenschutzgesetze informiert, geschult und angewiesen sind und sich schriftlich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Geheimhaltungspflicht unterliegen. Der Auftragsbearbeiter wird sich in wirtschaftlich angemessener Weise darum bemühen, dass diese befugten Personen die geltenden Datenschutzgesetze auch über ihre jeweilige Beschäftigungszeit hinaus in Bezug auf die relevanten Daten einhalten.
  5. Die technischen und organisatorischen Massnahmen umzusetzen, die den Anforderungen des geltenden Datenschutzrechts entsprechen, bevor er die relevanten Daten bearbeitet, und dem Verantwortlichen ausreichende Garantien für diese technischen und organisatorischen Massnahmen zu geben. Zu diesem Zweck verfügt der Auftragsbearbeiter über ein Managementsystem für die Informationssicherheit, das nach internationalen Standards und bewährten Verfahren gepflegt wird. Die Parteien sind sich darüber einig, dass die Verpflichtung zur Durchführung dieser technischen und organisatorischen Massnahmen strikt auf die Systeme, Prozesse und Infrastrukturen beschränkt ist, die unter der direkten Kontrolle des Auftragsbearbeiters stehen. Der Auftragsbearbeiter haftet nicht für Systeme, Verfahren und Infrastrukturen oder für Folgen, die sich aus der fehlender oder mangelhafter Compliance von Systemen, Verfahren und Infrastrukturen ergeben, die nicht der direkten Kontrolle des Auftragsbearbeiters unterstehen.
  6. Des Verantwortlichen durch geeignete technische und organisatorische Massnahmen zu unterstützen, soweit dies möglich ist, bei der Erfüllung der Verpflichtung des Verantwortlichen, auf Anfragen zur Ausübung der Rechte der betroffenen Personen in Bezug auf Auskunft, Zugang, Berichtigung und Löschung, Einschränkung der Bearbeitung, Benachrichtigung, Datenübertragbarkeit, Widerspruch und automatisierte Entscheidungsfindung zu reagieren.
  7. Massnahmen zu ergreifen, die der Verantwortliche verlangt oder anweist, um die Rechte der betroffenen Person nach dem geltenden Datenschutzrecht zu wahren. Insbesondere muss der Auftragsbearbeiter die Informationen über die auf ein solches Ersuchen hin ergriffenen Massnahmen ohne unangemessene Verzögerung bzw. rechtzeitig zur Verfügung stellen.
  8. Dem Verantwortlichen alle Informationen zur Verfügung zu stellen, die erforderlich sind für die Compliance mit diesem DPA sowie mit Art. 28 GDPR oder mit Art. 10a DSG, je nachdem, was der Fall ist.
  9. Audits zuzulassen und an ihnen mitzuwirken, die sich auf die Bewertung der Einhaltung dieses DPA beschränken. Die dem Auftragsbearbeiter im Zusammenhang mit einem solchen Audit entstandenen Kosten werden von dem Verantwortlichen erstattet. Etwaige Kosten Dritter im Zusammenhang mit einem solchen Audit sind von der Partei zu tragen, die verursacht hat. Ein solches Audit darf höchstens einmal pro Jahr und nur von einem unabhängigen Dritten, der sich in keinem Interessenkonflikt befindet, durchgeführt werden.
  10. Den Verantwortlichen ohne unnötige Verzögerung zu benachrichtigen:
      1. über jedes rechtsverbindliche Ersuchen einer Strafverfolgungsbehörde um Offenlegung der relevanten Daten, sofern dies nicht anderweitig untersagt ist, z. B. durch ein strafrechtliches Verbot zur Wahrung der Vertraulichkeit einer strafrechtlichen Untersuchung;
      2. über alle Beschwerden und Anfragen, die direkt von betroffenen Personen eingehen (z. B. in Bezug auf Auskunft, Berichtigung, Löschung, Einschränkung der Bearbeitung, Datenübertragbarkeit, Widerspruch gegen die Bearbeitung von Daten, automatisierte Entscheidungsfindung), ohne auf diese Anfrage zu reagieren, sofern nicht anderweitig dazu befugt;
      3. nachdem der Auftragsbearbeiter von einer Verletzung des Schutzes personenbezogener Daten beim Auftragsbearbeiter oder seinen Unterauftragsbearbeitern Kenntnis erlangt hat. Im Falle einer solchen Verletzung des Schutzes personenbezogener Daten unterstützt der Auftragsbearbeiter den Verantwortlichen bei der Untersuchung der Verletzung des Schutzes personenbezogener Daten und der Verpflichtung des Verantwortlichen nach dem anwendbaren Datenschutzrecht, die betroffenen Personen und gegebenenfalls die Aufsichtsbehörden zu informieren und die Verletzung des Schutzes personenbezogener Daten zu dokumentieren.
  11. Zur Unterstützung des Verantwortlichen bei der Durchführung von Datenschutz-Folgenabschätzungen und ggf. bei der vorherigen Konsultation, die sich auf die vom Auftragsbearbeiter für den Verantwortlichen erbrachten Dienstleistungen und die im Auftrag des Verantwortlichen bearbeiteten relevanten Daten beziehen.

# Weiterbearbeitung

* 1. Der Verantwortliche genehmigt die Beauftragung der verbundenen Unternehmen des Auftragsbearbeiters als Unterauftragsbearbeiter.
  2. Der Verantwortliche genehmigt ebenfalls die Beauftragung von Dritten als Unterauftragsbearbeiter, auf die im Angebot des Auftragsbearbeiters, in der Leistungsbeschreibung, im Vertrag, in der referenzierten Dokumentation oder auf Online-Seiten usw. Bezug genommen wird.
  3. Der Auftragsbearbeiter informiert den Verantwortlichen über alle beabsichtigten Änderungen in Bezug auf die Hinzufügung oder den Austausch von Unterauftragsbearbeitern und gibt dem Verantwortlichen die Möglichkeit, innerhalb von 90 Tagen Einspruch gegen diese Änderungen zu erheben; danach gilt der neue Unterauftragsbearbeiter als akzeptiert.
  4. Jeder Untervertrag mit einem Dritten, durch den eine Bearbeitung relevanter Daten in Auftrag gegeben wird, muss im Einklang mit dem anwendbaren Datenschutzrecht stehen.
  5. Der Auftragsbearbeiter muss vertraglich sicherstellen, dass der Unterauftragsbearbeiter in Bezug auf den untervergebenen Teil der Bearbeitung relevanter Daten gegenüber dem Auftragsbearbeiter Verpflichtungen hat, die denen des Auftragsbearbeiters gegenüber dem Verantwortlichen entsprechen, insbesondere, dass der Unterauftragsbearbeiter ausreichende Garantien dafür bietet, dass er geeignete technische und organisatorische Massnahmen so umsetzt, dass die Bearbeitung den Anforderungen des geltenden Datenschutzrechts entspricht.
  6. Kommt ein Unterauftragsbearbeiter seinen Datenschutzverpflichtungen nicht nach, so bleibt der Auftragsbearbeiter gegenüber dem Verantwortlichen in vollem Umfang für die Erfüllung der Verpflichtungen des Unterauftragsbearbeiters haftbar.
  7. Falls ein solcher Unterauftragsbearbeiter ausserhalb Europas in einem Land ansässig ist, das von der Aufsichtsbehörde nicht als Land anerkannt ist, das ein angemessenes Datenschutzniveau bietet, vereinbart der Auftragsbearbeiter mit dem betreffenden Unterauftragsbearbeiter die entsprechenden SCC.

# Laufzeit und Beendigung

* 1. Die Laufzeit dieser DPA ist identisch mit der Laufzeit der jeweiligen Vereinbarung bzw. im Falle laufender/nachfolgender Geschäftsbeziehungen unter verschiedenen Verträgen identisch mit der längsten Laufzeit dieser Verträge.
  2. Der Auftragsbearbeiter löscht nach Wahl des Verantwortlichen alle relevanten Daten nach Beendigung der Erbringung der Dienstleistungen oder gibt sie an den Verantwortlichen zurück und löscht alle vorhandenen Kopien. Der Auftragsbearbeiter kann eine Kopie der personenbezogenen Daten zu Beweiszwecken und/oder zur Begründung, Ausübung oder Verteidigung von Rechtsansprüchen und/oder zur Einhaltung der geltenden Gesetze und Vorschriften aufbewahren.

# Zahlung

* 1. Alle Beträge, die für die vom Auftragsbearbeiter erbrachten Dienstleistungen zu zahlen sind, sowie die Zahlungsbedingungen sind in der Vereinbarung niedergelegt. Im Zusammenhang mit diesem DPA sind keine weiteren Zahlungen oder sonstigen Gegenleistungen zu erbringen, es sei denn, in diesem DPA ist ausdrücklich etwas anderes festgelegt.
  2. Die Auslagen müssen dem Auftragsbearbeiter erstattet werden.

# Geltendes Recht

* 1. Dieses DPA unterliegt schweizerischem Recht und ist nach diesem auszulegen, unter Ausschluss der Kollisionsnormen und ungeachtet des Ortes dessen physischen Ausführung oder Erfüllung.

# Zuständigkeitsbereich

* 1. Für Streitigkeiten im Zusammenhang mit diesem DPA sind ausschliesslich die ordentlichen Gerichte von Bern zuständig, ohne dass dadurch das Recht auf Berufung eingeschränkt wird. Ungeachtet dessen ist jede Vertragspartei jedoch befugt, bei jeder zuständigen Behörde weltweit einstweilige Verfügungen und Unterlassungsmassnahmen zu beantragen.

# Sonstiges

* 1. Sollte eine der Bestimmungen dieses DPA unwirksam sein oder werden, so wird dadurch die Wirksamkeit des DPA im Ganzen nicht berührt. An die Stelle der unwirksamen oder nichtigen Bestimmung tritt diejenige wirksame Bestimmung, die die Parteien vereinbart hätten, wenn sie die Unwirksamkeit zum Zeitpunkt des Abschlusses des DPA gekannt hätten, um das gleiche wirtschaftliche Ergebnis zu erzielen.
  2. Dieses DPA stellt die gesamte Übereinkunft der Parteien in Bezug auf den Gegenstand dieser Vereinbarung dar und ersetzt alle früheren schriftlichen oder mündlichen Vereinbarungen, Verhandlungen oder Diskussionen zwischen den Parteien vor der Unterzeichnung dieser Vereinbarung, unabhängig davon, ob diese ausdrücklich oder stillschweigend erfolgten.

# Definitionen

* 1. **"Europäisches Datenschutzrecht"** bezeichnet alle Datenschutzgesetze und Vorschriften, die in Europa anwendbar sind, sowie deren Ergänzungen und Revisionen wie auch deren Ausführungsverordnungen, einschliesslich **(**i) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Bearbeitung personenbezogener Daten und zum freien Datenverkehr ("**DSGVO**"); (ii) die Richtlinie 2002/58/EG über die Bearbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation; (iii) die anwendbaren nationalen Umsetzungen von (i) und (ii); (iv) das Schweizerische Bundesgesetz über den Datenschutz vom 25. September 2020 ("**DSG**")**;** und (v) in Bezug auf das Vereinigte Königreich ("**UK**") alle anwendbaren nationalen Rechtsvorschriften, die die DSGVO oder andere Gesetze in Bezug auf Daten und den Schutz der Privatsphäre infolge des Austritts der UK aus der Europäischen Union ersetzen oder in nationales Recht umwandeln;
  2. **"Europa"** bezeichnet für die Zwecke dieses DPA die Europäische Union, den Europäischen Wirtschaftsraum und/oder ihre Mitgliedstaaten, die Schweiz und die UK.
  3. **"Anwendbares Datenschutzrecht"** bezeichnet die Gesetze und Vorschriften innerhalb der europäischen Datenschutzgesetze, die die Pflichten der jeweiligen Partei und ihre Bearbeitungstätigkeit regeln und auf diese Anwendung finden.
  4. **"Aufsichtsbehörde"** bezeichnet eine unabhängige öffentliche Behörde, die gemäss dem europäischen Datenschutzgesetz eingerichtet wurde, z. B. gemäss Artikel 51 der DSGVO oder, in Bezug auf die Schweiz, der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte.
  5. **"Technische und organisatorische Massnahmen"** sind Massnahmen zum Schutz personenbezogener Daten vor zufälliger Zerstörung, zufälligem Verlust, zufälliger Änderung, unberechtigter Weitergabe oder unberechtigtem Zugriff, insbesondere wenn die Bearbeitung die Übermittlung von Daten über ein Netz umfasst, sowie vor jeder anderen Form der unrechtmässigen Bearbeitung.
  6. **"SCC"** bezeichnet die von der Europäischen Kommission oder einer Aufsichtsbehörde in Europa (je nach Anwendbarkeit) genehmigten Standardvertragsklauseln zur Absicherung von Übermittlungen personenbezogener Daten zur Bearbeitung an Empfänger in Ländern, die von der zuständigen Behörde nicht als ein angemessenes Datenschutzniveau im Sinne des europäischen Datenschutzrechts anerkannt sind.
  7. **"Verbundene(s) Unternehmen"** bedeutet jede in- oder ausländische Gesellschaft, die zum Zeitpunkt der Unterzeichnung dieses DPA gegründet wurde und die direkt oder indirekt von der betreffenden Partei oder ihrer Muttergesellschaft kontrolliert wird oder an der die betreffende Partei oder ihre Muttergesellschaft direkt oder indirekt mindestens 50 % des Aktienkapitals hält.
  8. **"Relevante Daten"** sind personenbezogene Daten, die vom Auftragsbearbeiter im Auftrag des Verantwortlichen auf der Grundlage der Vereinbarung im Zusammenhang mit der Erbringung der Dienstleistungen bearbeitet werden.
  9. **"Betroffene Person(en)", "personenbezogene Daten", "Verantwortlicher", "Auftragsbearbeiter", "Unterauftragsbearbeiter", "Verletzung des Schutzes personenbezogener Daten", "Bearbeitung", "besondere Datenkategorien"** haben die gleiche Bedeutung wie in der DSGVO.

# Unterschriften

Die unterzeichnenden Parteien stimmen dieses DPA, datiert vom Datum des Inkrafttretens, und ihren Bedingungen zu.

Die Parteien vereinbaren, dass dieses DPA in Papierform durch handschriftliche Unterschriften oder alternativ in elektronischer Form durch Standards für elektronische Signaturen mit rechtsverbindlicher Wirkung gemäss den geltenden Rechtsvorschriften ausgefertigt werden kann.

**xxx-AG:**

Ort und Datum:

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

Unterschrift Unterschriftsberechtigter Unterschrift Unterschriftsberechtigter

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

Name in Blockbuchstaben Name in Blockbuchstaben

**SPIE ICS AG:**

Ort und Datum:

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

Unterschrift Unterschriftsberechtigter Unterschrift Unterschriftsberechtigter

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

Name in Blockbuchstaben Name in Blockbuchstaben

Annex 2: Technische und Organisatorische Massnahmen des Auftragsbearbeiters

*Der Auftragsbearbeiter führt hier eine abschliessende Liste von Massnahmen zum Schutz der Daten auf und kann auch auf etwaige Zertifizierungs- oder Managementsysteme für Informationssicherheit oder Datenschutz verweisen.*

1. Vertraulichkeit

## Zugang

*Massnahmen, die geeignet sind, Unbefugten den Zugang zu Datenbearbeitungssystemen zu verwehren, mit denen personenbezogene Daten Bearbeitet oder genutzt werden. Als Zutrittskontrollmassnahmen für die Gebäude- und Raumsicherheit können unter anderem automatische Zutrittskontrollsysteme, der Einsatz von Chipkarten und Transpondern, die Zutrittskontrolle durch Pförtner und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Systeme müssen in abschliessbaren Serverschränken geschützt werden. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle mit Organisatorischen Massnahmen zu unterstützen (z.B. Dienstanweisungen, die das Abschliessen der Büros bei Abwesenheit vorsehen).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technische Massnahmen** | | **Organisatorische Massnahmen** | |
|  | Alarm |  | Schlüsselregelung / -liste |
|  | Automatisches Zutrittskontrollsystem |  | Rezeption / Empfang / Portier |
|  | Biometrische Zutrittsschlösser |  | Gästebuch / Besucherprotokoll |
|  | Chipkarten / Transpondersysteme |  | Mitarbeiter- /Besucherbadges |
|  | Manuelles Verriegelungssystem |  | Begleitung von Besuchern durch Mitarbeiter |
|  | Sicherheitsschlösser |  | Sorgfalt bei der Auswahl des Sicherheitspersonals |
|  | Schliesssystem mit Codeschloss |  | Sorgfalt bei der Auswahl der Reinigungsdienstleistern |
|  | Schutz der Bauschächte |  |  |
|  | Türen mit Knauf an der Aussenseite |  |  |
|  | Klingelanlage mit Kamera |  |  |
|  | Videoüberwachung der Eingänge |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Weitere/weitere Massnahmen:

## Physische Zugangskontrolle

*Massnahmen, die geeignet sind, die Nutzung von Datenbearbeitungssystemen (Computern) durch Unbefugte zu verhindern.*

*Unter Zutrittskontrolle versteht man die Verhinderung der unbefugten Nutzung von Geräten. Möglichkeiten sind z.B. Boot-Passwort, Benutzerkennung/-ID mit Passwort für verwendete Betriebssysteme und Softwareprodukte, Bildschirmschoner mit Passwort, die Verwendung von Chipkarten für das Login sowie die Nutzung von Rückrufverfahren. Darüber hinaus können auch Organisatorische Massnahmen erforderlich sein, um z.B. unbefugte Zugriffe zu verhindern (z.B. Vorgaben für die Installation von Bildschirmen, Hinweise an die Nutzer zur Wahl eines "guten" Passworts).*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technische Massnahmen** | | **Organisatorische Massnahmen** | |
|  | Login mit Benutzername + Passwort |  | Verwalten von Benutzerberechtigungen |
|  | Login mit Benutzername + Passwort + zweiter Faktor |  | Erstellen von Benutzerprofilen |
|  | Login mit biometrischen Daten |  | Zentrale Passwortvergabe |
|  | Antivirensoftware Server |  | Richtlinie für starke Passwörter |
|  | Antivirensoftware-Clients |  | "Löschen/Zerstören"-Richtlinie |
|  | Antivirensoftware für mobile Geräte |  | Clean-Desk-Richtlinie |
|  | Firewall |  | Allgemeine Datenschutz- und/oder Sicherheitsrichtlinie |
|  | Intrusion Detection Systeme |  | Richtlinie für mobile Geräte |
|  | Verwaltung mobiler Geräte |  | Anleitung für manuelle Desktop-Sperren |
|  | Verwendung von VPN für den Fernzugriff |  |  |
|  | Verschlüsselung von Datenträgern |  |  |
|  | Verschlüsselung Smartphones |  |  |
|  | Gehäuse-Verriegelung |  |  |
|  | BIOS-Schutz (separates Passwort) |  |  |
|  | Blockieren externer Schnittstellen (USB) |  |  |
|  | Automatische Desktop-Sperre |  |  |
|  | Verschlüsselung von Notebooks / Tablets |  |  |
|  |  |  |  |

Weitere/weitere Massnahmen:

## Zugriffskontrolle

*Massnahmen, die sicherstellen, dass die zur Nutzung eines Datenbearbeitungssystems berechtigten Personen nur gemäss ihrer Zugriffsberechtigung auf Daten zugreifen können und dass Personendaten während der Bearbeitung, der Nutzung und nach der Speicherung nicht unbefugterweise gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem durch geeignete Berechtigungskonzepte sichergestellt werden, die eine differenzierte Steuerung der Datenzugriffe ermöglichen. Dabei ist es wichtig, zwischen dem Inhalt der Daten und den möglichen Zugriffsfunktionen auf die Daten zu unterscheiden. Des Weiteren sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Widerruf von Berechtigungen zu dokumentieren und aktuell zu halten (z.B. bei Einstellung, Arbeitsplatzwechsel, Beendigung des Arbeitsverhältnisses). Besonderes Augenmerk muss stets auf die Rolle und die Möglichkeiten der Administratoren gelegt werden.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technische Massnahmen** | | **Organisatorische Massnahmen** | |
|  | Aktenvernichter (min. Stufe 3 / DIN 3, Querschnitt) |  | Verwendung von Berechtigungskonzepten |
|  | Externer Aktenvernichter (DIN32757) |  | Mindestanzahl von Administratoren |
|  | Physisches Löschen von Festplatten |  | Privacy Vault |
|  | Protokollierung der Zugriffe auf Anwendungen, insbesondere beim Eingeben, Ändern und Löschen von Daten |  | Verwaltung von Benutzerrechten durch Administratoren |
|  |  |  |  |
|  |  |  |  |

Weitere/weitere Massnahmen:

## Trennungskontrolle

*Massnahmen, die sicherstellen, dass Daten, die für unterschiedliche Zwecke erhoben werden, getrennt Bearbeitet werden können. Dies kann z.B. durch eine logische und physische Trennung der Daten sichergestellt werden.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technische Massnahmen** | | **Organisatorische Massnahmen** | |
|  | Trennung von Produktions- und Testumgebung |  | Steuerung gemäss Berechtigungskonzept |
|  | Physikalische Trennung (Systeme / Datenbanken / Datenträger) |  | Ermittlung von Datenbankrechten |
|  | Mehr-Mandantenfähigkeit relevanter Anwendungen |  | Datensätze werden mit Zweckattributen versehen |
|  |  |  |  |
|  |  |  |  |

Weitere/weitere Massnahmen:

## Anonymisierung / Pseudonymisierung / Verschlüsselung

*Die Bearbeitung von Personendaten erfolgt in der Art, dass die Daten nicht mehr einer bestimmten Betroffenen Person zugeordnet werden können, ohne Hinzuziehung zusätzlicher Informationen - unter der Voraussetzung, dass diese zusätzlichen Informationen separat gespeichert werden und geeigneten technischen und Organisatorischen Massnahmen unterliegen.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technische Massnahmen** | | **Organisatorische Massnahmen** | |
|  | Im Falle der Pseudonymisierung:  Trennung von Auftragsdaten und Speicherung in einem separaten und sicheren System (wenn möglich verschlüsselt) |  | Interne Weisung zur weitestgehenden Anonymisierung / Pseudonymisierung Personendaten im Falle einer Offenlegung oder auch nach Ablauf der gesetzlichen Löschfrist |
|  | Die Daten sind anonymisiert und können nicht einer einzelnen Person zugeordnet werden. |  |  |
|  | Verschlüsselung |  |  |
|  |  |  |  |

Weitere/weitere Massnahmen:

1. Integrität

## Weitergabe-Kontrolle

*Massnahmen, die sicherstellen, dass Personendaten während der elektronischen Übertragung, des Transports oder der Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen Personendaten über Datenübertragungseinrichtungen übermittelt werden sollen. Um die Vertraulichkeit bei der elektronischen Datenübertragung zu gewährleisten, können z.B. Verschlüsselungstechniken und virtuelle private Netze (VPN) eingesetzt werden. Massnahmen für den Datenträgertransport bzw. die Datenübertragung sind Transportbehälter mit Verriegelungsvorrichtungen und Vorschriften zur datenschutzkonformen Vernichtung von Datenträgern.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technische Massnahmen** | | **Organisatorische Massnahmen** | |
|  | Verschlüsselung von Daten |  | Dokumentation der Datenempfänger sowie der Dauer der geplanten Übermittlung bzw. der Löschfristen |
|  | Verwendung von VPN |  | Übersicht über den regulären Abruf und  Übermittlungsvorgänge |
|  | Protokollierung von Zugriffen und Abrufen |  | Weitergabe in anonymisierter oder pseudonymisierter Form |
|  | Sichere Transportbehälter |  | Sorgfalt bei der Auswahl von Transportpersonal und Fahrzeugen |
|  | Bereitstellung über verschlüsselte Verbindungen wie sftp, https |  | Persönliche Übergabe mit Protokoll |
|  | Verwendung von Signaturverfahren |  | Die Wahl eines zuverlässigen Transporters |
|  |  |  |  |
|  |  |  |  |

Weitere/weitere Massnahmen:

## Eingabekontrolle

*Massnahmen, die sicherstellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Personendaten eingegeben, verändert oder aus Datenbearbeitungssystemen entfernt wurden. Die Eingabekontrolle wird durch ein Logging/Protokollierung erreicht, das auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) erfolgen kann. Zu klären ist auch, welche Daten protokolliert werden, wer Zugriff auf die Protokolle/Logs hat, von wem und zu welchem Anlass/Zeitpunkt diese überprüft werden, wie lange eine Speicherung erforderlich ist und wann die Protokolle/Logs gelöscht werden.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technische Massnahmen** | | **Organisatorische Massnahmen** | |
|  | Technische Protokollierung der Eingabe, Änderung und Löschung von Daten |  | Übersicht, mit welchen Programmen welche Daten erfasst, geändert oder gelöscht werden können |
|  | Manuelle oder automatisierte Kontrolle von Protokollen |  | Nachvollziehbarkeit von Eingaben, Änderungen und Löschungen von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) |
|  | Protokollierung von Administratoraktivitäten |  | Vergabe von Rechten zum Eingeben, Ändern und Löschen von Daten auf Basis eines Berechtigungskonzepts |
|  | Schutz der Protokolldaten vor Verlust oder Veränderung |  | Aufbewahrung von Formularen, aus denen Daten in die automatisierte Bearbeitung übernommen wurden |
|  |  |  | Klare Verantwortlichkeiten für Löschungen |
|  |  |  |  |

Weitere/weitere Massnahmen:

# Verfügbarkeit und Ausfallsicherheit

## Verfügbarkeits-Check

*Massnahmen, um sicherzustellen, dass Personendaten vor versehentlicher Zerstörung oder Verlust geschützt sind. Dabei geht es um Themen wie unterbrechungsfreie Stromversorgung, Klimatisierung, Brandschutz, Datensicherung, sichere Aufbewahrung von Datenträgern, Virenschutz, Raid-Systeme, Disk Mirroring, etc.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technische Massnahmen** | | **Organisatorische Massnahmen** | |
|  | Brand- und Rauchmeldeanlagen |  | Backup & Recovery-Konzept (formuliert) |
|  | Feuerlöscher im Serverraum |  | Kontrolle des Backup-Prozesses |
|  | Überwachung der Temperatur und Luftfeuchtigkeit im Serverraum |  | Regelmässige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse |
|  | Klimatisierter Serverraum |  | Lagerung der Sicherungsmedien an  einem sicheren Ort ausserhalb des  Serverraum |
|  | Unterbrechungsfreie Stromversorgung |  | Keine sanitären Anschlüsse im oder  über dem Serverraum |
|  | Schutzsteckdosenleisten im Serverraum |  | Vorliegen eines Notfallplans (z.B. BSI IT-Grundschutz 100-4) |
|  | Privacy Vault (S60DIS, S120DIS,  andere geeignete Normen mit Quelldichtungen, etc.) |  | Separate Partitionen für Betriebssysteme und Daten |
|  | RAID-System / Disk Mirroring |  |  |
|  | Videoüberwachung Serverraum |  |  |
|  | Alarmmeldung bei unbefugtem Zutritt zum Serverraum |  |  |
|  |  |  |  |
|  |  |  |  |

Weitere/weitere Massnahmen:

# Periodische Überprüfung, Beurteilung und Evaluierungsverfahren

## Datenschutz-Management

|  |  |  |  |
| --- | --- | --- | --- |
| **Technische Massnahmen** | | **Organisatorische Massnahmen** | |
|  | Softwarelösungen für das Datenschutz-Management in Anwendung |  | Interner/externer Datenschutzbeauftragter:  Name / Firma / Kontaktdaten |
|  | Zentrale Dokumentation aller Vorgänge und Regelungen zum Datenschutz mit Zugang für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...) |  | Mitarbeiter geschult und zur Vertraulichkeit/zu Datengeheimnis verpflichtet |
|  | Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12 |  | Regelmässige Sensibilisierung der Mitarbeiter, mindestens einmal pro Jahr |
|  | Sonstiges dokumentiertes Sicherheitskonzept |  | Interner / externer Informationssicherheitsbeauftragter:  Name / Firma / Kontakt |
|  | Eine Überprüfung der Wirksamkeit der technischen Schutzmassnahmen erfolgt mindestens einmal jährlich |  | Die Datenschutz-Folgenabschätzung (DSFA) wird erforderlichenfalls durchgeführt |
|  |  |  | Die Organisation kommt den Informationspflichten gemäss Art. 13 und 14 DSGVO nach |
|  |  |  | Formalisiertes Verfahren für die Bearbeitung von Auskunftsersuchen Betroffener Personen ist vorhanden |
|  |  |  |  |
|  |  |  |  |

Weitere/weitere Massnahmen:

## Incident-Response-Management

*Unterstützung bei der Reaktion auf Sicherheitsverletzungen*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technische Massnahmen** | | **Organisatorische Massnahmen** | |
|  | Verwendung von Firewall mit regelmässiger Aktualisierung |  | Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datensicherheitsverletzungen (auch im Hinblick auf Meldepflichten gegenüber der Aufsichtsbehörde) |
|  | Verwendung von Spam-Filtern inkl. regelmässiger Updates |  | Dokumentiertes Vorgehen im Umgang mit Sicherheitsvorfällen |
|  | Einsatz von Virenscanner inkl. regelmässiger Updates |  | Involvierung von DPO und ISBs bei Sicherheitsvorfällen und Datensicherheitsverletzungen |
|  | Intrusion Detection System (IDS) |  | Dokumentation von Sicherheitsvorfällen und Datensicherheitsverletzungen, z.B. via Ticketsystem |
|  | Intrusion Prevention System (IPS) |  | Formaler Prozess und Zuständigkeiten für die Nachverfolgung von Sicherheitsvorfällen und Datensicherheitsverletzungen |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Weitere/weitere Massnahmen:

## Datenschutzfreundliche Einstellungen

*Datenschutz durch Design (Privacy by design) / Datenschutz als Standard (privacy by default)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technische Massnahmen** | | **Organisatorische Massnahmen** | |
|  | Es werden nicht mehr Personendaten erhoben, als für den jeweiligen Zweck erforderlich |  |  |
|  | Einfache Ausübung des Widerrufsrechts der von technischen Massnahmen betroffenen Personen |  |  |
|  |  |  |  |
|  |  |  |  |

Weitere/weitere Massnahmen:

## Kontrolle von Aufträgen

*Massnahmen, die sicherstellen, dass Personendaten, die im Auftrag des Kunden bearbeitet werden, ausschliesslich gemäss den Weisungen des Kunden bearbeitet werden können. Dazu gehört neben der Datenbearbeitung im Auftrag des Kunden auch die Durchführung von Wartungs- und Systemsupportarbeiten sowohl vor Ort als auch aus der Ferne. Setzt der Auftrgsbearbeiter im Sinne der Auftragsabwicklung Dienstleister/Unterauftragsnehmer ein, so sind mit diesen stets die folgenden Punkte zu regeln.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Technische Massnahmen** | | **Organisatorische Massnahmen** | |
|  |  |  | Vorherige Prüfung der vom Unterauftragsbearbeiter getroffenen Sicherheitsmassnahmen und dessen Dokumentation |
|  |  |  | Verpflichtung der Mitarbeiter des Unterauftragsbearbeiter zur Wahrung des Datengeheimnisses |
|  |  |  | Pflicht zur Benennung eines Datenschutzbeauftragten (DPO) durch den Unterauftragsbearbeiter im Falle einer Benennungspflicht |
|  |  |  | Vereinbarung über wirksame Kontrollrechte für den Auftrasbearbeiter |
|  |  |  | Vorgaben über den Einsatz von zusätzlichen Unterauftragsbearbeiter |
|  |  |  | Sicherstellung der Vernichtung von Daten nach Abschluss des Auftrags |
|  |  |  |  |
|  |  |  |  |

Weitere/weitere Massnahmen:

**xxx-AG:**

Ort und Datum:

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

Unterschrift Zeichnungsberechtigter Unterschrift Zeichnungsberechtigter

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

Name in Druckbuchstaben Name in Druckbuchstaben

# Annex 1 – Einzelheiten zur Bearbeitung

**Der im Vertrag/Kundenvertrag definierte Gegenstand umfasst folgende Bearbeitungen**

|  |
| --- |
|  |

*(Geben Sie den Gegenstand des Vertrags/der Kundenvereinbarung oder eine Beschreibung der vereinbarten und zu erbringenden Dienstleistungen an.)*

**Art und Zweck der Bearbeitung**

|  |
| --- |
|  |

*(Genauere Beschreibung, ggf. Verweis auf Vertrag/Kundenvereinbarung).*

**Ort der Bearbeitung**

|  |
| --- |
|  |

*(Wo werden die personenbezogenen Daten Bearbeitet und/oder wo kann auf die Personendaten zugegriffen werden? Gegebenenfalls ist der Verweis auf "zugelassene Unterauftragnehmer" anzugeben.*

**Dauer der Bearbeitung**

|  |
| --- |
|  |

*(Wie lange werden die Daten Bearbeitet, während und nach Beendigung des Vertrages und wie werden die Daten gelöscht).*

**Kategorien und Art der personenbezogenen Daten**

|  |
| --- |
|  |

*(Welche personenbezogenen Datenkategorien werden Bearbeitet und welche Art von Daten)*

**Datenübertragungen**

|  |
| --- |
|  |

*(An wen erfolgt die Datenübermittlung und welche Schutzmassnahmen wurden getroffen. Beschreibung der Massnahmen für die Übermittlung oder den Zugang zu diesen Ländern, Drittland und in welchen Ländern)*

**Verantwortlicher: Ansprechpartner für den Datenschutz oder DPO**

|  |
| --- |
|  |

*(Name, Funktion, Telefonnummer, E-Mail, Adresse)*

**SPIE: Ansprechpartner für Datenschutz**

|  |
| --- |
| 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:**

Ort und Datum:

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

Unterschrift Zeichnungsberechtigter Unterschrift Zeichnungsberechtigter

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

Name in Druckbuchstaben Name in Druckbuchstaben

**SPIE ICS AG:**

Ort und Datum:

Unterschrift Zeichnungsberechtigter Unterschrift Zeichnungsberechtigter

Eduardo GERALDI Name in Druckbuchstaben