Vereinbarung zur Verarbeitung von personenbezogenen Daten im Auftrag gemäß Art. 28 DSGVO

- Auftraggeber (EPLAN Vertragspartner) und Auftragnehmer (EPLAN GmbH & Co. KG) jeweils auch als „**Partei**“ und gemeinsam als „**Parteien**“ bezeichnet -

Diese Vereinbarung zur Auftragsverarbeitung (**„AV“**) konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus der im Zusammenhang mit der Nutzung der EPLAN Cloud verbundenen Verarbeitung personenbezogener Daten im Auftrag (nachfolgend auch **„Hauptvertrag“**) gemäß Art. 28 der Verordnung (EU) 2016/679 **(„DSGVO“)** ergeben.
Diese AV findet auf nachfolgend genannte Tätigkeiten und/oder Personenkreise, die mit der Ausführung dieser Tätigkeiten im Zusammenhang mit dem Hauptvertrag zur Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers **(„Daten des Auftraggebers“)** betraut sind, Anwendung:

- auf Mitarbeiter des Auftragnehmers und/oder vom Auftragnehmer beauftragte Dritte, die mit personenbezogenen Daten, für die der Auftraggeber „Verantwortlicher“ im Sinn der DSGVO ist, in Berührung kommen, oder
- hinsichtlich der Verarbeitung personenbezogener Daten durch Mitarbeiter des Auftragnehmers, bei welcher der Auftraggeber selbst – da er personenbezogene Daten im Auftrag eines Dritten verarbeitet - Auftragsverarbeiter i.S.d. DSGVO ist und den Auftragnehmer als Unterauftragsverarbeiter einsetzt.

1. Definitionen

Für die in dieser AV verwendeten Begriffe gelten die Definitionen in Art. 4 DSGVO, es sei denn, sie werden ausdrücklich abweichend definiert. Eine Liste der für diese AV besonders relevanten Definitionen ist in **Anlage zu Ziff. 1 - Definitionen** aufgeführt.

2. Vertragsbestandteile und Rangordnung

(1) Die AV ist mit ihren Anlagen unmittelbarer und verbindlicher Bestandteil des Hauptvertrags. Sie hat im Zweifel Vorrang vor Regelungen des Hauptvertrags, es sei denn, in dieser AV oder einer Anlage wurde ausdrücklich etwas Abweichendes festgelegt.
Die in dieser AV einschließlich der Anlagen aufgeführten Verpflichtungen zum Datenschutz stellen für den Auftragnehmer wesentliche Vertragspflichten (Hauptpflichten)dar.

(2) Im Fall von Lücken oder Widersprüchen gilt folgende absteigende Rangordnung, anhand welcher der Vertragsinhalt ermittelt wird, wobei die Anlagen zur AV untereinander ranggleich sind:

- AV (dieses Dokument)
- Anlagen zur AV
- Hauptvertrag samt Anlagen

Für die Bestimmung des Rangs vom Hauptvertrag und den Anlagen des Hauptvertrags gilt die im Hauptvertrag getroffene Regelung. Ist dort keine Regelung getroffen, wird für die Auslegung dieser AV davon ausgegangen, dass die Anlagen des Hauptvertrags dem Hauptvertrag vorgehen.

3. Festlegung von Gegenstand, Art und Zweck der Auftragsverarbeitung

(1) Der Auftragnehmer verarbeitet die Daten des Auftraggebers ausschließlich im Rahmen des Auftrags und nur auf dokumentierte Weisung (Ziff. 4) des Auftraggebers.

(2) Der Auftraggeber ist im Rahmen dieser AV für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer, die Rechtmäßigkeit der Datenverarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich.

(3) Der Gegenstand der Auftragsverarbeitung folgt aus dem Hauptvertrag, insbesondere aus einer ggf. vorhandenen Leistungsbeschreibung. Soweit der Hauptvertrag keine oder keine hinreichende Beschreibung zum Gegenstand der Auftragsverarbeitung enthält, haben die Parteien den Gegenstand der Auftragsverarbeitung in der Anlage **zu Ziff. 3 –Festlegung von Gegenstand, Art und Zweck der Auftragsverarbeitung** näher spezifiziert.

(4) Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen sind ebenfalls näher in **Anlage zu Ziff. 3 – Festlegung von Gegenstand, Art und Zweck der Auftragsverarbeitung** beschrieben, wenn sich dies nicht aus dem Hauptvertrag ergibt.

(5) Die Bestimmungen dieser AV gelten entsprechend, soweit Gegenstand, Art und Zweck der Tätigkeit des Auftragnehmers die auch über administrativen Zugriff erfolgende, Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen ist, und dabei ein Zugriff auf personenbezogenen Daten nicht ausgeschlossen werden kann.

4. Weisungen des Auftraggebers

(1) Die Verarbeitung personenbezogener Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen, es sei denn es liegt eine gesetzlich angeordnete Ausnahme nach Art. 28 Abs. 3 lit. a DSGVO vor. Auskünfte an betroffene Personen oder an Dritte darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen.

(2) Weisungen bedürfen der Schrift- oder Textform und nur ausnahmsweise sind in Eilfällen mündliche Weisungen zulässig. In diesem Fall werden die Weisungen im Anschluss vom Auftraggeber unverzüglich in Schrift- oder Textform dokumentiert und dem Auftragnehmer übermittelt.

(3) Der Auftragnehmer hat Weisungen grundsätzlich vorbehaltslos und unverzüglich nach Maßgabe folgender Bestimmungen umzusetzen:

- Der Auftragnehmer wird den Auftraggeber vor Ausführung der Weisung darüber informieren, wenn die Erteilung einer Weisung z.B. zur Löschung von Daten des Auftraggebers nach Einschätzung des Auftragnehmers dazu führt, dass der Auftragnehmer seine unter dem jeweiligen Hauptvertrag geschuldeten Produkte oder Leistungen nicht mehr bereitstellen kann, oder dass ein Zugriff auf die Leistungen, z.B. das Einloggen auf Nutzerkonten, unmöglich wird. Bestätigt der Auftraggeber die Weisung, erfolgt dies auf Gefahr des Auftraggebers und dieser kann dem Auftragnehmer

eine dadurch eventuell verursachte Einschränkung der Leistungen des Auftragnehmers nicht entgegenhalten.

- Ist der Auftragnehmer der Meinung, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften, hat er den Auftraggeber unverzüglich in Schrift- oder Textform zu informieren. In diesem Fall ist der Auftragnehmer berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(4) Die Kommunikation zwischen den Parteien ist ausschließlich über die Emailadresse: Digitale-plattform@eplan.de zu führen.

(5) Im Übrigen sind Einwendungen, Einreden oder Zurückbehaltungsrechte in Bezug auf die Daten des Auftraggebers und deren Verarbeitung ausgeschlossen.

(6) Der Auftragnehmer verwendet die Daten des Auftraggebers für keine anderen Zwecke als die, zu denen der Auftraggeber Weisungen erteilt hat, und ist insbesondere nicht berechtigt, die Daten des Auftraggebers ohne dessen Weisung an Dritte weiterzugeben oder deren Zugriff zu dulden. Kopien und Duplikate der Daten des Auftraggebers werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind im ordentlichen Betriebsgang erstellte Sicherheitskopien, oder die Speicherung von Daten des Auftraggebers, soweit dies zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich ist.

(7) Weisungen, die inhaltlich über den im Hauptvertrag festgelegten Leistungsumfang hinausgehen und nicht der datenschutzrechtlichen Konkretisierung bestehender Leistungspflichten dienen, sind für den Auftragnehmer nicht verbindlich i.S.v. Ziff. 4 (3), sondern bedürfen zu ihrer Wirksamkeit der ausdrücklichen Vereinbarung zwischen den Parteien. Ist im Hauptvertrag ein förmliches Änderungsverfahren für Leistungs- und/oder Vertragsänderungen geregelt, ist dieses entsprechend zu berücksichtigen.

5. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer wird in seinem Verantwortungsbereich und für die Dauer dieser AV die nach Art. 32 DSGVO erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung ergreifen. Dabei wird der Auftragnehmer seine innerbetriebliche Organisation unter Berücksichtigung

- des jeweiligen Stands der Technik,
- der Implementierungskosten,
- der Art, des Umfangs sowie der Umstände und Zwecke der Verarbeitung und
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen

so gestalten, dass sie den besonderen Anforderungen des Datenschutzes nach der DSGVO entsprechen und den Schutz der Rechte der Betroffenen Personen gewährleisten.

(2) Die zu ergreifenden technisch-organisatorischen Maßnahmen umfassen insbesondere

- die auf Dauer angelegte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der Daten,
- die Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- die Möglichkeit zur raschen Wiederherstellung der Verfügbarkeit personenbezogener

Daten und den Zugang zu ihnen im Fall eines physischen oder technischen Zwischenfalls,
- die Einführung und das Vorhalten von Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(3) Der Auftragnehmer hat die von ihm ergriffenen Maßnahmen dokumentiert und sie als **Technisch-organisatorische Maßnahmen** zu diesem Vertrag hinzugenommen. Siehe Anlage zu Ziff. 5.

(4) Die vom Auftragnehmer ergriffenen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Dem Auftragnehmer ist es gestattet, alternative und adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der bisher festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber zur Prüfung vorzulegen. Dabei ist die **Technisch-organisatorische Maßnahmen** des Auftragnehmers vom Auftragnehmer mindestens einmal jährlich und auf Aufforderung des Auftraggebers daraufhin zu überprüfen, ob diese die getroffenen Maßnahmen noch adäquat wiedergibt, andernfalls ist sie zu aktualisieren.

(5) Der Auftragnehmer kann die Geeignetheit der - insbesondere nach Art. 32 DSGVO zu treffenden - technisch-organisatorischen Maßnahmen durch einen Nachweis über

- die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO; oder
- die Einhaltung eines genehmigten Zertifizierungsverfahrens nach Art. 42 DSGVO

belegen. Dazu genügt die Vorlage eines Zertifikates einer akkreditierten Zertifizierungsstelle nach Art. 43 DSGVO; eine Kopie des Zertifikats wird dann ebenfalls als Technisch-**organisatorische Maßnahmen des Auftragnehmers** zum Vertrag genommen. Die Vorlage einer Zertifizierung beschränkt nicht die Verantwortlichkeit des Auftragnehmers für das Vorhandensein eines angemessenen Schutzniveaus bzw. entsprechender Garantien.

(6) Der Auftraggeber behält sich vor, die Einhaltung der in Ziff. 5 (1) bis 5 (5) genannten Maßnahmen im Rahmen seiner Audit- und Kontrollrechte (Ziff. 13) zu überprüfen.

6. Rechte betroffener Personen, Unterstützungsleistungen

(1) Der Auftraggeber ist für die Wahrung der Rechte der betroffenen Person nach dem III. Kapitel der DSGVO verantwortlich. Werden solche Rechte unmittelbar gegenüber dem Auftragnehmer geltend gemacht, hat der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterzuleiten. Dies gilt nur, soweit dem Auftragnehmer eine Zuordnung zur betroffenen Person möglich ist. Ist dem Auftragnehmer eine Zuordnung nicht möglich, unterrichtet der Auftragnehmer den Auftraggeber entsprechend Art. 11 Abs. 2 DSGVO über die fehlende Identifizierbarkeit und die Gründe dafür.

(2) Werden Ersuchen von betroffenen Personen nicht unverzüglich weitergeleitet, haftet der Auftragnehmer dem Auftraggeber für etwaige Verzögerungen bei der Bearbeitung von Anfragen von betroffenen Personen unter Berücksichtigung der in Art. 12 Abs. 3 DSGVO genannten Bearbeitungsfristen, es sei denn, der Auftragnehmer hat die Verzögerung nicht zu vertreten.

(3) Dem Auftragnehmer ist die Umsetzung der Rechte betroffener Personen, etwa eines Löschbegehrens, nur nach Weisung des Auftraggebers gestattet.

(4) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erfüllung von Anfragen und Ansprüche betroffener Personen nach dem III. Kapitel der DSGVO vollumfänglich zu unterstützen und hierzu im erforderlichen Umfang Personal und Betriebsmittel zur Verfügung zu stellen.

7. Verpflichtung auf das Datengeheimnis

(1) Der Auftragnehmer gewährleistet, dass die beim Auftragnehmer mit der Verarbeitung der Daten des Auftraggebers betrauten Beschäftigten

- Daten des Auftraggebers nicht außerhalb der Weisungen des Auftraggebers verarbeiten;
- über ihre Pflichten zur Wahrung des Datenschutzes, zur vertraulichen Behandlung der Daten des Auftraggebers sowie zur Wahrung von Vertraulichkeit belehrt wurden; und
- einer entsprechenden persönlichen Verpflichtungserklärung über Datenschutz, Wahrung der Vertraulichkeit sowie über die Pflicht zur Verschwiegenheit unterliegen.

Entsprechendes gilt für weitere datenschutzrechtliche Vertraulichkeits- und/oder Schutzbestimmungen, soweit einschlägig (z.B. ein gesetzlich geregeltes Berufsgeheimnis). Die Vertraulichkeit-/Verschwiegenheitspflicht muss auch nach Beendigung der Tätigkeit der betreffenden Beschäftigten für den Auftragnehmer fortbestehen.

(2) Die Belehrung und Verpflichtung der betrauten Beschäftigten gemäß Ziff. 7 (1) ist dem Auftraggeber auf Verlangen geeignet nachzuweisen (z.B. Mustererklärung).

(3) Der Auftragnehmer kann seine Pflicht nach Ziff. 7 (1) auch durch den Nachweis über die Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO) oder den Nachweis über die Einhaltung eines genehmigten Zertifizierungsverfahrens (Art. 42 DSGVO) erbringen, soweit hieraus hervorgeht, dass die bei der Verarbeitung eingesetzten Beschäftigten nach Ziff. 7 (1) verpflichtet sind.

8. Meldung von Datenschutzverstößen

(1) Der Auftragnehmer erstattet dem Auftraggeber in allen Fällen und ohne Rücksicht auf die Zuordnung eines eventuellen Verschuldens Meldung, wenn der Auftragnehmer

- von einer tatsächlichen Verletzung des Schutzes personenbezogener Daten durch den Auftragnehmer oder durch einen seiner Beschäftigten, oder
- von einem Verstoß gegen gesetzliche Vorschriften zum Schutz personenbezogener Daten oder
- von einem Verstoß gegen die in dieser Vereinbarung getroffenen Festlegungen

Kenntnis erlangt (jeweils ein „**Datenschutzvorfall**“). Die Meldung des Datenschutzvorfalls an den Auftraggeber hat unverzüglich, aber spätestens innerhalb von 36 Stunden ab Kenntniserlangung zu erfolgen.

(2) Die Meldung eines Datenschutzvorfalls hat – soweit zum Zeitpunkt der Kenntniserlangung möglich - sämtliche Informationen zu enthalten, die der Auftraggeber zur Erfüllung seiner Pflichten nach Art. 33 und Art. 34 DSGVO benötigt; insbesondere

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

- den Namen und die Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers, oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, zur Verhinderung zukünftiger Vorfälle, und, gegebenenfalls, Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(3) Sobald der Auftragnehmer Kenntnis von einem Datenschutzvorfall erhält, trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Abmilderung nachteiliger Auswirkungen für die betroffenen Personen und den Auftraggeber. Sofern dazu Weisungen des Auftraggebers erforderlich sind, holt er diese ein.

(4) Der Auftragnehmer ist verpflichtet, Datenschutzvorfälle ausführlich zu dokumentieren, einschließlich deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Die Dokumentation ist dem Auftraggeber unverzüglich zur Verfügung zu stellen.

(5) Sofern der Datenschutzvorfall nicht vom Auftragnehmer zu vertreten ist, findet für die Aufwände des Auftragnehmers im Rahmen dieser Ziff. 8, Ziff. (5) entsprechende Anwendung.

9. Ort der Datenverarbeitung und Drittländer

(1) Die Verarbeitung der Daten erfolgt ausschließlich in

- einem Mitgliedsstaat der Europäischen Union (EU); oder
- einem Nicht-EU Mitgliedsstaat des Hauptabkommens über den Europäischen Wirtschaftsraum vom 2. Mai 1992 („EWR-Abkommen“) sobald dieser die DSGVO gem. Art. 102 Abs. 1 EWR-Abkommen übernommen hat; oder
- in einem Staat, für welches es einen Angemessenheitsbeschluss der EU-Kommission (Art. 45 Abs. 3 DSGVO) gibt.

Jede Verarbeitung von Daten außerhalb der vorgenannten Territorien bedarf der vorherigen Zustimmung des Auftraggebers.

(2) Die Zustimmung setzt voraus, dass für die in Frage kommende Verarbeitung die besonderen Voraussetzungen der Art. 44 ff. DSGVO dauerhaft erfüllt sind.

10. Unterauftragnehmer

(1) Die Einbeziehung weiterer Auftragsverarbeiter durch den Auftragnehmer („**Unterauftragnehmer**“) ist zulässig, wenn folgende Voraussetzungen kumulativ erfüllt sind:

- Die Beauftragung von Unterauftragnehmern werden vom Auftragnehmer rechtzeitig angekündigt und auf der EPLAN Homepage unter Third-Party (eplan.com). und in der Anlage zu dieser Ziffer 10 dargestellt. Dem Auftraggeber sind dabei auf Anforderung geeignete Nachweise über die im Folgenden aufgeführten Maßnahmen vorzulegen.
- Der Auftragnehmer hat den Unterauftragnehmer sorgfältig gewählt und vor Beauftragung daraufhin geprüft, ob der Unterauftragnehmer die zwischen dem Auftraggeber und dem Auftragnehmer getroffenen Vereinbarungen, insbesondere diese AV, zuverlässig, fachlich, technisch und organisatorisch einhalten kann.
- Der Auftragnehmer hat seine vertraglichen Vereinbarungen mit dem Unterauftragnehmer so gestaltet, dass diese den Datenschutzbestimmungen im

Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer, insbesondere dieser AV, mindestens entsprechen, wobei der Unterauftragnehmer insbesondere hinreichende datenschutzrechtliche Garantien i.S.d. DSGVO dafür geboten hat, dass dieser geeignete technische und organisatorische Maßnahmen so durchführt, dass die Verarbeitung entsprechend der Anforderungen der DSGVO erfolgt. Der Auftragnehmer darf zu diesem Zweck die für den Datenschutz relevanten Abschnitte der zwischen Auftraggeber und Auftragnehmer geltenden vertraglichen Vereinbarung, insbesondere der AV, gegenüber dem Unterauftragnehmer offenlegen.

- Dem Auftraggeber werden vom Unterauftragnehmer unmittelbare Weisungs-, Kontroll- und Überprüfungsrechte entsprechend Art. 28 Abs. 3 lit. f. DSGVO i.V.m. Ziff. 13 dieser AV eingeräumt (i.S. eines echten Vertrags zugunsten Dritter). Die genannten Weisungs-, Kontroll- und Überprüfungsrechte gelten auch zu Gunsten eines etwaigen Auftraggebers des Auftraggebers, sowie für jegliche Aufsichtsbehörden, die für den Auftraggeber, einen Auftraggeber des Auftraggebers, den Auftragnehmer, oder den Unterauftragnehmer zuständig sind.
- Der Auftragnehmer wird das Unterauftragsverhältnis vertraglich so gestalten, dass der Auftragnehmer dem Auftraggeber auf dessen Verlangen Rechte aus dem Unterauftragsverhältnis auf den Auftraggeber übertragen kann und/oder den Auftraggeber dahingehend bevollmächtigen, dass der Auftraggeber die Rechte des Auftragnehmers aus dem Unterauftragsverhältnis wahrnehmen kann.

(2) Die Weitergabe von Daten des Auftraggebers an den Unterauftragnehmer und die Aufnahme der Verarbeitungstätigkeit sind erst mit Vorliegen aller in Ziff. 10 (1) genannten Voraussetzungen zulässig.

(3) Im Tagesgeschäft kontaktiert der Auftraggeber einen Unterauftragnehmer nur nach Rücksprache mit dem Auftragnehmer, der Auftragnehmer übernimmt die Koordination sämtlicher Verlangen des Auftraggebers mit dem Unterauftragnehmer, und leitet entsprechende Rückmeldungen oder Berichte weiter.

(4) Der Auftragnehmer informiert den Auftraggeber per Benachrichtigungsfunktion in der EPLAN CLOUD mindestens 4 Wochen im Voraus über die Aufnahme von weiteren Unterauftragsverarbeitern. Ausgenommen sind die mit dem Auftragnehmer verbundenen Unternehmen, die als Unterauftragnehmer eingesetzt werden dürfen, wenn der Auftragnehmer den Auftraggeber vor deren erstem Einsatz darüber unterrichtet, insofern erteilt der Auftraggeber eine hiermit allgemeine Genehmigung i.S.d. Art. 28 Abs. 2 Satz 1 DSGVO.

(5) Soweit der Auftraggeber mit dem Einsatz eines Unterauftragnehmers nicht einverstanden ist, steht ihm ein Sonderkündigungsrecht zu. Das Sonderkündigungsrecht muss innerhalb eins Zeitraums von 4 Wochen nach Ankündigung der Zusammenarbeit mit dem Unterbeauftragten auf der EPLAN Homepage in Textform ausgeübt werden. Wird das Sonderkündigungsrecht nicht innerhalb dieser Frist ausgeübt, wird die Zustimmung des Auftraggebers mit der Unterbeauftragung fingiert. Im Falle der fristgerechten Ausübung des Sonderkündigungsrechts wird die Kündigung zum Zeitpunkt des Beginns der Unterbeauftragung wirksam.

(6) Nicht als Unterauftragsverhältnisse im Sinne dieser Ziff. 10 sind solche Leistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, oder Prüfer.

11. Herausgabe und Löschung von Daten und Datenträgern

(1) Der Auftraggeber kann seine Daten jederzeit selbst exportieren.

(2) Der Auftragnehmer wird nach Beendigung der AV und davor jederzeit auf Verlangen des Auftraggebers sämtliche in seinen Besitz gelangte Unterlagen, überlassene Datenträger, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen oder im Rahmen der Vertragsdurchführung entstanden sind, an den Auftraggeber oder an einen vom Auftraggeber benannten Dritten herausgeben, oder, auf den ausdrücklichen Wunsch des Auftraggebers hin, löschen. Die Bereitstellung hat auf Verlangen des Auftraggebers in einem industrieüblichen Standardformat zu erfolgen.
Die Herausgabepflicht umfasst auch Kopien und/oder Reproduktionen von Datenträgern und/oder Datenbeständen. Ein Zurückbehaltungsrecht besteht nicht. Die Herausgabe hat einwende- sowie einredefrei zu erfolgen. Etwaige Kosten für die Übermittlung sowie sonstige, mit der Herausgabe im Zusammenhang stehende, Aufwendungen sind vom Auftragnehmer zu tragen, Ziff. 6 (5) gilt entsprechend.

(3) Nach Herausgabe der Daten gem. Ziff. 11 (1) oder wenn der Auftraggeber die Löschung anordnet, sind die auf den Datenträgern des Auftragnehmers ggf. noch vorhandenen Daten einer datenschutzgerechten Vernichtung bzw. Löschung zuzuführen. Die endgültige Löschung der Daten setzt das Einverständnis des Auftraggebers voraus. Der Auftragnehmer hat dem Auftraggeber auf Verlangen die Durchführung der Löschung durch geeignete Dokumente und/oder einer entsprechenden Eigenerklärung nachzuweisen.
Ist der Auftragnehmer aufgrund von gesetzlichen Bestimmungen zu einer Aufbewahrung von Daten oder Materialien verpflichtet, die Daten des Auftraggebers enthalten, erfolgt eine Einschränkung der Verarbeitung. Die fraglichen Daten oder Materialien dürfen ausschließlich zum Zweck der Erfüllung der Aufbewahrungspflichten verwendet werden und werden vom Auftragnehmer für andere Zwecke gesperrt. Derartige Materialien und personenbezogene Daten werden vom Auftragnehmer in einer Weise verwahrt, die während der Dauer ihrer Aufbewahrung mindestens den Anforderungen dieser AV entspricht, unbeschadet einer Beendigung der AV oder des Hauptvertrags. Nach Ablauf der entsprechenden Fristen werden die betreffenden Daten oder Materialien im Rahmen des gewöhnlichen Geschäftsgangs des Auftragnehmers vernichtet. Satz 1 dieser Ziff. 11 (2) gilt entsprechend.
Entsprechendes gilt, wenn die Löschung der Daten und Materialien auf technischer Ebene aufgrund der besonderen Speicherart nicht mit angemessenem technischen oder zeitlichen Aufwand, oder auf wirtschaftlicher Ebene nur zu unverhältnismäßig hohen Kosten möglich ist.

(4) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Ende dieser AV hinaus aufzubewahren. Der Auftragnehmer kann sich davon entlasten, indem er zum Ende der AV dem Auftraggeber eine Dokumentation übergibt.

(5) Die Regelungen der Ziffern 11 (1) und 11 (2) gelten für Test- und Ausschussmaterial entsprechend. Die Kosten der Vernichtung trägt der Auftraggeber.

12. Weitere Pflichten des Auftragnehmers

(1) Der Auftragnehmer wird die für das vom Auftraggeber nach Art. 30 DSGVO zu führende Verzeichnis der Verarbeitungstätigkeiten erforderlichen Angaben und Informationen zur beauftragten Verarbeitung bereitstellen. Die Bereitstellung hat auf Verlangen des Auftraggebers und in einem industrieüblichen, bearbeitbaren Standardformat zu erfolgen.

(2) Der Auftragnehmer wird den Auftraggeber bei der Einhaltung der Pflichten nach Art. 32 DSGVO beraten und unterstützen. Hierzu wird der Auftragnehmer dem Auftraggeber die für die Dokumentation der Maßnahmen nach Art. 32 DSGVO erforderlichen Unterlagen, Dokumente und Nachweise zur Verfügung stellen. Die im Laufe der Durchführung der AV

anfallenden Aktualisierungen dieser Materialien reicht der Auftragnehmer unaufgefordert nach.

(3) Der Auftragnehmer wird dem Auftraggeber bei der Durchführung und Einhaltung der Datenschutz-Folgeabschätzung nach Art. 35 DSGVO beraten und unterstützen.

(4) Sofern rechtlich zulässig, ist der Auftraggeber über alle den Auftragnehmer und die Daten des Auftraggebers betreffenden Kontrollhandlungen und Maßnahmen einer Aufsichtsbehörde, insbesondere nach Art. 58 DSGVO, unverzüglich zu informieren. Dies gilt auch, wenn eine zuständige Behörde beim Auftragnehmer ermittelt.

(5) Der Auftragnehmer ist verpflichtet, im Hinblick auf die Durchführung bzw. Erfüllung dieser AV die Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags regelmäßig zu überprüfen. Der Auftragnehmer wird den Auftraggeber unverzüglich über dabei gefundene Fehler und/oder Unregelmäßigkeiten informieren und dessen Entscheidung einholen.

(6) Soweit gesetzlich vorgeschrieben, wird der Auftragnehmer einen Datenschutzbeauftragten, der seine Tätigkeit uneingeschränkt gemäß Art. 37, 38, 39 DSGVO ausüben kann, bestellen. Der Auftragnehmer teilt dem Auftraggeber unaufgefordert die Kontaktdaten des Datenschutzbeauftragten oder - soweit ein Datenschutzbeauftragter nicht zu bestellen ist - eines anderen entscheidungsbefugten Ansprechpartners für Datenschutzfragen zum Zweck der direkten Kontaktaufnahme mit, ebenso wie jede Änderung davon.

(7) Sollten Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, sofern gesetzlich zulässig. Der Auftragnehmer wird alle in diesem Zusammenhang verantwortlichen Personen unverzüglich darüber in Kenntnis setzen, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ liegen.

13. Kontroll- und Prüfungsrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder im Einzelfall durch zur Verschwiegenheit verpflichtete Dritte bzw. Prüfer durchführen zu lassen. Der Auftraggeber hat insbesondere das Recht, sich durch Stichprobenkontrollen von der Einhaltung dieser AV im Geschäftsbetrieb des Auftragnehmers zu dessen üblichen Geschäftszeiten zu überzeugen.
(2) Das Vorliegen entsprechender Verschwiegenheitsvereinbarungen ist dem Auftragnehmer auf Verlangen geeignet nachzuweisen. Berufsständische Verschwiegenheitspflichten sind ausreichend, soweit sie gesetzlich strafbewehrt sind, z.B. Rechtsanwälte, Steuerberater. Der Auftragnehmer kann einen Prüfer nur dann ablehnen, wenn die betreffende Person für einen unmittelbaren Wettbewerber des Auftragnehmers tätig ist. Von Aufsichtsbehörden zum Auftraggeber oder einen Auftraggeber des Auftraggebers entsendete Prüfer bedürfen keiner besonderen Verschwiegenheitsvereinbarung; ein Ablehnungsrecht besteht nicht.
(3) Kontrollen sind in der Regel mit einer Vorlaufzeit von vierzehn (14) Tagen anzukündigen. In dringenden Fällen kann der Auftraggeber die Ankündigungsfrist auf 24 Stunden abkürzen. Ein dringender Fall liegt insbesondere dann vor, wenn

- konkrete Anhaltspunkte dafür bestehen, dass der Auftragnehmer laufend gegen gesetzliche Bestimmungen zum Datenschutz oder gegen diese AV verstößt,

- konkrete Anhaltspunkte dafür bestehen, dass aufgrund eines Verstoßes des Auftragnehmers gegen gesetzliche Bestimmungen zum Datenschutz oder gegen diese AV eine Notifizierungspflicht des Auftraggebers nach Art. 33 DSGVO oder einer anderen gesetzlichen Bestimmung besteht, oder
- der Auftraggeber oder ein Auftraggeber des Auftraggebers Gegenstand einer Inspektion oder Prüfung einer Datenschutzaufsichtsbehörde oder sonstigen Aufsichtsbehörden ist und der Gegenstand der Inspektion oder Prüfung auch den Auftragnehmer betrifft.

(4) Der Auftragnehmer gewährleistet, dass der Auftraggeber und die von ihm beauftragten Prüfer sich von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28, 29 DSGVO in Bezug auf die vertragsgegenständliche Verarbeitung von Daten des Auftraggebers im Auftrag überzeugen können. Der Auftragnehmer wird dem Auftraggeber alle erforderlichen Auskünfte erteilen und insbesondere die Umsetzung der technisch- organisatorischen Maßnahmen gemäß Art. 32 DSGVO nachweisen.

(5) Die Unterstützungsleistungen des Auftragnehmers bei der Durchführung von Kontrollen (z.B. Aufwendungen, Personal) sind im Umfang von einer Kontrolle/Jahr sowie bei durch schuldhaftes Verhalten des Auftragnehmers oder bei von Aufsichtsbehörden veranlassten Kontrollen mit der Vergütung aus dem Hauptvertrag abgegolten. Der Auftraggeber kann die genannten Kontroll- und Audit-Rechte während der Laufzeit der AV sowie für einen Zeitraum von drei Jahren nach der Beendigung der AV ausüben.

14. Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

(2) Der Auftraggeber wird den Auftragnehmer unverzüglich und vollständig informieren, wenn er bei Prüfung der Verarbeitungsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Dem Auftraggeber obliegt die Pflicht zur Führung eines öffentlichen Verfahrensregisters nach Art. 30 DSGVO. Die Verpflichtung des Auftragnehmers zur Führung eines eigenen Verfahrensregisters nach Art. 30 Abs. 2 DSGVO bleibt hiervon unberührt.

(4) Der Auftraggeber benennt einen für die im Rahmen der AV anfallenden Datenschutzfragen zuständigen Ansprechpartner und teilt dem Auftragnehmer die Kontaktdaten zum Zweck der direkten Kontaktaufnahme mit.

15. Dauer, Kündigung, Beendigung

(1) Diese AV tritt mit Unterzeichnung durch beide Parteien in Kraft und läuft auf unbestimmte Zeit. Sie endet grundsätzlich mit Beendigung des Hauptvertrages, wobei, soweit der Hauptvertrag nachvertragliche Pflichten vorsieht, die die Verarbeitung von Daten des Auftraggebers umfassen, die AV erst mit Beendigung dieser Pflichten endet. Es bedarf keiner gesonderten Kündigungserklärung.
(2) Der Auftraggeber kann die AV einschließlich des Hauptvertrages mit sofortiger Wirkung außerordentlich kündigen, wenn

- der Auftragnehmer schuldhaft gegen gesetzliche Bestimmungen zum Datenschutz und/oder gegen Verpflichtungen aus dieser AV verstößt und dem Verstoß trotz Mahnung nicht innerhalb von dreißig (30) Kalendertagen abhilft; oder

- der Auftragnehmer schuldhaft gegen gesetzliche Bestimmungen zum Datenschutz und/oder gegen Verpflichtungen aus dieser AV verstößt, und die Auswirkung des Verstoßes zu einem Schaden oder Haftungsansprüchen Dritter oder einer Bußgeldpflicht des Auftraggebers in Höhe von mehr als EUR 10.000,00 führt; oder
- der Auftragnehmer schuldhaft gegen nach Ziff. 5 zu ergreifende technisch-organisatorische Maßnahmen verstößt und es dadurch zu einer wesentlichen Verletzung der Sicherheit der Daten des Auftraggebers kommt.

(3) Eine Beendigung der AV – gleich aus welchem Grund – führt dazu, dass jede der Parteien berechtigt ist, diejenigen Leistungen unter dem jeweiligen Hauptvertrag, die eine Verarbeitung von Daten des Auftraggebers erfordern, solange auszusetzen, bis die Parteien sich über das weitere Vorgehen, z.B. den Abschluss einer Folge-AV oder die Beendigung des Hauptvertrags, verständigt haben. Leistungen, bei denen keine Daten des Auftraggebers verarbeitet werden, sind weiter zu erbringen. Ansprüche wegen der Leistungseinstellung, insbesondere Schadensersatz oder auf Kürzung einer laufenden Vergütung, sind ausgeschlossen.

16. Allgemeine Bestimmungen

(1) Bei der Verarbeitung der Daten des Auftraggebers und der Auslegung der Anforderungen der DSGVO sowie der Bestimmungen dieser AV werden die Parteien die Empfehlungen der Art. 29 Datenschutzgruppe oder deren Nachfolgeorganisation (Europäischer Datenschutzausschuss) angemessen berücksichtigen. Im Zweifel bestimmt sich anhand der Empfehlungen was die vom Auftragnehmer zu erreichende mittlere Art und Güte der vom Auftragnehmer geschuldeten Leistungen sein muss.

(2) Die Parteien sind sich einig, die vorliegende Vereinbarung einschließlich ihrer Anlagen anzupassen und/oder zu ändern, soweit dies in Folge von Änderungen, Anpassungen und/oder Ergänzungen gesetzlicher Bestimmungen – insbesondere der DSGVO und/oder der jeweils anwendbaren nationalen Datenschutzbestimmungen – erforderlich ist. Änderungen erfolgen, sofern nicht abweichend in dieser AV bestimmt, stets einvernehmlich. Ist im Hauptvertrag ein förmliches Änderungsverfahren geregelt, kann jede der Parteien verlangen, dass dieses auch auf Änderungen dieser AV angewendet wird.

(3) Im Übrigen wird vereinbart, dass die Parteien einander rechtzeitig unterrichten, wenn sie der Ansicht sind, eine Änderungen der rechtlichen Vorschriften zum Datenschutz berühre die Pflichten des Auftragnehmers gegenüber dem Auftraggeber unter dieser AV oder dem jeweiligen Hauptvertrag und mache eine Änderung der AV oder einer der Anlagen erforderlich. Die Parteien werden eine gegenseitig annehmbare Lösung herbeiführen und dabei auch die Auswirkungen dieser Maßnahme auf die vereinbarte Vergütung berücksichtigen.
Im Übrigen gelten die Bestimmungen des Hauptvertrags.

Anlagenverzeichnis:
- Anlage zu Ziff. 1 - Definitionen
- Anlage zu Ziff. 3 - Festlegung von Gegenstand, Art und Zweck der Auftragsverarbeitung
- Anlage zu Ziff. 5 - Technisch-organisatorische Maßnahmen des Auftragnehmers
- Anlage zu Ziff. 10 - Unterauftragnehmer

Anlage zu Ziff. 1 – Definitionen

„**Auftragsverarbeiter**“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Im Zusammenhang mit dieser AV ist der Auftragnehmer Auftragsverarbeiter, jedoch kann auch der Auftraggeber seinerseits Auftragsverarbeiter eines dritten Auftraggebers sein.

Als „**Beschäftigter**“ gelten

- Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,
- zu ihrer Berufsbildung Beschäftigte, einschließlich Praktikanten,
- Teilnehmerinnen und Teilnehmer an staatlich geregelten Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
- in staatlich anerkannten Werkstätten für behinderte Menschen Beschäftigte,
- Freiwillige, die einen gesetzlich geregelten Freiwilligendienst leisten,
- Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
- Beamtinnen und Beamte, Richterinnen und Richter, Soldatinnen und Soldaten sowie Zivildienstleistende, unabhängig davon, bei welcher staatlichen Stelle sie beschäftigt sind.

Ebenso gelten Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, als Beschäftigte.

„**Besondere Kategorien personenbezogener Daten**“ sind personenbezogene Daten i.S.d. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische und biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

„**Dritter**“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

„**Einwilligung**“ der betroffenen Person meint jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

„**Personenbezogene Daten**“ bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (die „**betroffene Person**“) beziehen. Als „identifizierbar“ wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

„**Verantwortlicher**“ meint die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen sein. Im Zusammenhang mit dieser Vereinbarung ist der Verantwortliche der Auftraggeber. Der Auftraggeber kann seinerseits Auftragsverarbeiter eines dritten Verantwortlichen sein.

„**Verarbeitung**“ meint einen mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang, oder eine Reihe von Vorgängen, im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

„**Verbundene Unternehmen**“ im Sinne dieser AV sind rechtlich selbstständige Unternehmen, die a) die Mehrheit der Anteile oder die Mehrheit der Stimmrechte an einem anderen Unternehmen haben (Mehrheitsbeteiligung) sowie solche Unternehmen, die unter einer solchen Mehrheitsbeteiligung stehen, oder b) die auf ein anderes Unternehmen unmittelbar oder mittelbar einen beherrschenden Einfluss ausüben können (Beherrschungsverhältnis) sowie solche Unternehmen, die unter einem solchen Beherrschungsverhältnis stehen, oder c) die unter einer gemeinsamen Leitung geführt werden oder in sonstiger Abhängigkeit zueinander stehen (Konzernverhältnis).

„**Weisung**“ ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) an den Auftragnehmer gerichtete Weisung des Auftraggebers. Die Weisungen werden durch den Hauptvertrag festgelegt und können vom Auftraggeber danach durch einzelne, den Hauptvertrag konkretisierende Weisungen (Einzelweisung) nach diesem Vertrag ergänzt werden.

Anlage zu Ziff. 3 – Festlegung von Gegenstand, Art und Zweck der Auftragsverarbeitung

1. Gegenstand, Art und Zweck der Auftragsverarbeitung

EPLAN bietet den Kunden die Nutzung der EPLAN Cloud an, auf der Mitarbeiter des Kunden nach Anlage eines Accounts und der damit verbundenen Speicherung der Accountdaten (wie in den EPLAN Cloud Nutzungsbedingungen beschrieben) mit internen und externen Kollegen im Engineering Prozess zusammenarbeiten und Daten austauschen können. Innerhalb der EPLAN Cloud Plattform hat der Kunde eine eigene gekapselte, Organisation genannte, Einheit, zu welcher er über die E-Mail-Adresse Anwender einladen und für den Zugriff auf Daten und Applikationen autorisieren kann.

2. Art der personenbezogenen Daten

Folgende Datenarten / -kategorien sind Gegenstand der Auftragsverarbeitung:
☒ Personenstammdaten
☒ Kommunikationsdaten (z.B. Telefon, E-Mail)

3. Kategorien betroffener Personen

Folgende Kategorien von Betroffenen sind von der Auftragsverarbeitung betroffen:
☒ Kunden
☒ Beschäftigte des Kunden
☒ Lieferanten des Kunden

4. Orte der Verarbeitung

Microsoft Azure Datenzentren innerhalb der EU

Anlage zu Ziff. 5 – Technisch-organisatorische Maßnahmen des Auftragnehmers

1. Zusammenfassung

Gemäß Art. 32 der EU-Datenschutzgrundverordnung (DSGVO) sind alle Stellen, welche personenbezogene Daten erheben, verarbeiten und nutzen, verpflichtet, sogenannte technisch- organisatorische Maßnahmen (nachfolgend „TOMs“ genannt) zu treffen, um zu gewährleisten, dass die Anforderungen der DSGVO erfüllt sind.

Die Rittal Software Systems GmbH & Co. KG (nachfolgend „RSS“ genannt) ist ein Unternehmensverbund der Schwesterfirmen EPLAN GmbH und Co. KG und der CIDEON Software & Services GmbH & Co. KG der Friedhelm Loh Group (nachfolgend „FLG“ genannt) und hat für sich und ihre verbundenen Unternehmen nachfolgende TOMs zur internen und externen Anwendung definiert.

Die hierin niedergelegten Maßnahmen werden insbesondere aus Sicherheitsgründen, d.h. zur Minimierung von Sicherheitsrisiken bzgl. des Zugriffs auf Unternehmensdaten und entsprechender Wahrung von Betriebs- und Geschäftsgeheimnissen, nicht im Detail offengelegt, sondern dienen lediglich als grundsätzliche Maßgabe, um den o.g. Anforderungen zu genügen.

Diese TOMs, folgen im Aufbau den Anforderungen von Art. 32 DSGVO und der zugehörigen Anlage.

2. Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Zutrittskontrolle

Die RSS trifft Maßnahmen der Zutrittskontrolle, um zu verhindern, dass Unbefugte Zutritt (räumlich) zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden. Dies umfasst:

- Gebäudesicherung
  - Zäune; Türen/Tore
  - Empfangspersonal
  - Videoüberwachung
  - Besucherausweise und Besucherliste
  - Sicherheitsdienste außerhalb der Geschäftszeiten
- Sicherung der Räume
  - Sicherheitsschlösser
  - Chipkartenleser
  - Codeschlösser
  - Sicherheitsverglasung
  - Alarmanlagen

Die Server-Betriebsräume der RSS sind in mehrere Sicherheitsbereiche mit differenzierten Zugangsberechtigungen aufgeteilt. Diese werden außerhalb der Geschäftszeiten durch einen Sicherheitsdienst überwacht.

Der Zutritt zu den Gebäuden der RSS ist (außerhalb der üblichen Geschäftszeiten) nur mit codierten Mitarbeiterausweisen mit entsprechender Berechtigung bzw. Schlüssel, die an die entsprechend berechtigten Mitarbeiter ausgehändigt wurden, möglich sowie für diejenigen beauftragen Personen der RSS, die über eine entsprechende schriftlich erteilte Berechtigung und Ausweise bzw. Schlüssel verfügen. Während der üblichen Geschäftszeiten werden Besucher durch das Empfangspersonal in Besucherlisten erfasst und durch Übergabe von Besucherausweisen als Besucher kenntlich gemacht.

Außerhalb der üblichen Bürozeiten empfangene Besucher werden individuell durch den einladenden Mitarbeiter betreut.

Server- und/oder Technikräume sind mit herkömmlichen Schließsystemen gesichert und nur für definierte verantwortliche Mitarbeiter der RSS-IT zugänglich.

Für Gebäude bzw. Räume der RSS, die mit Alarmanlagen ausgestattet sind, erhalten nur diejenigen Mitarbeiter des jeweiligen Standortes einen Aktivierungs- bzw. Deaktivierungsschlüssel, die einen solchen Zutritt zur Erfüllung Ihrer dienstlichen Aufgaben benötigen. Innerhalb der einzelnen Sicherheitsbereiche sind je nach Sicherheitsstufe Maßnahmen wie Sicherheitsschlösser oder zusätzliche elektronische Kartenlesegeräte vorhanden.

Alle Mitarbeiter haben ihren Mitarbeiterausweis sichtbar am Körper zu tragen. Die Mitarbeiterausweise sind mindestens mit dem Namen des Mitarbeiters versehen sowie der Angabe ihrer organisatorischen Zugehörigkeit innerhalb der RSS.

Besucher müssen idealerweise im Vorfeld beim Empfang angemeldet werden, jedenfalls ist der Zutritt zu den Gebäuden der RSS für Besucher ausschließlich nach Anmeldung beim Empfang gestattet. Besucher sind verpflichtet ihre Identität mit einem Lichtbildausweis nachzuweisen, ihren vom Empfang ausgehändigten Besucherausweis jederzeit gut sichtbar am Körper zu tragen und sich nur in Begleitung von Mitarbeitern der RSS im Gebäude zu bewegen.

2.2 Zugangskontrolle

Die RSS trifft Maßnahmen zur Zugangskontrolle, um zu verhindern, dass Unbefugte Zugang zu den Datenverarbeitungsanlagen (nachfolgend „DV-Anlagen“ genannt) erhalten. Dies umfasst:

- Sicherung des Zugangs zu Rechnern/Systemen (Authentifizierung)
  - Benutzerkennung mit Passwort und Passwortrichtlinie gemäß der gültigen Kennwortrichtlinie (u.a. Sonderzeichen, Mindestlänge),
  - biometrische Benutzeridentifikation,
  - Firewall,
  - zertifikatsbasierte Zugangsberechtigung,
  - Verschlüsselung von Zugängen ins Netzwerk mittels VPN,
  - Automatische Sperrung (z.B. Kennwort oder Pausenschaltung, Zeitablauf),
  - Verschlüsselung von Datenträgern (z.B. Bitlocker)

Der Zugang zu Client-Systemen im Netz der RSS ist nur über eine passwortgestützte Netzwerk-Authentifizierung möglich. Die dafür geltende Passwortrichtlinie regelt u.a. das Kennwortverfahren (Mindestlänge, Komplexität, Kennwortchronik). Die Protokollierung der Passwortnutzung erfolgt in Log-Files der individuellen Systeme - soweit vorhanden.

Der direkte Zugang von Extern (d.h. von außerhalb des RSS Netzwerks) ist ausschließlich über gesicherte und verschlüsselte Verbindungen und mit Security-Token sowie einem von der RSS zur Verfügung gestellten Rechner/Laptop (o.ä. Hardware) (nachfolgend „RSS-Rechner“ genannt“) möglich; andere oder sonstige angemessene Zugriffsmöglichkeiten sind in Ausnahmefällen nach schriftlicher Zustimmung durch die RSS möglich. Zusätzlich ist es Partnern und Dienstleistern möglich, auf einen Teil der IT-Systeme, gefiltert über ein SSL Portal (Reverse Proxy und z.B. Secure Application Manager) zuzugreifen.

Für den sicheren Zugang auf Drittsysteme werden Firewalls und Proxyserver eingesetzt. Falls eine Verschlüsselung des Übertragungsweges zum Kunden (VPN) erforderlich ist, wird diese in gemeinsamer Abstimmung nach aktuellem Stand der Technik und auf Basis des Abschlusses entsprechender Geheimhaltungs- sowie Datenverarbeitungsvereinbarungen eingerichtet.

2.3 Zugriffskontrolle

a) Allgemeine Maßnahmen

Die RSS hat Maßnahmen ergriffen, damit die zur Benutzung der DV-Anlagen berechtigten Nutzer ausschließlich auf solche Inhalte zugreifen können, zu deren Nutzung sie auch berechtigt sind. Darüber hinaus soll dadurch gewährleistet werden, dass im Rahmen der Verarbeitung, Speicherung und Nutzung personenbezogener Daten auf DV-Anlagen der RSS diese personenbezogenen Daten weder unbefugt verändert noch kopiert oder gelöscht werden können. Dies umfasst:

- Berechtigungskonzept
- Benutzerkennung mit Passwort
- gesicherte Schnittstellen (USB, Firewire, Netzwerk, etc.)
- Datenträgerverwaltung
- zertifikatsbasierte Zugriffsberechtigung.
- Einbindung in Mitarbeiter-Onboarding/Offboarding-Prozesse sowie regelmäßige Prüfung, ob Rechte noch benötigt werden

Es liegt ein RSS-Berechtigungskonzept mit einer entsprechenden Definition von Nutzerprofilen und Rollen hinsichtlich aller RSS-IT-Systemen zugrunde. Generell werden Berechtigungen nach dem „least-privileged“ Prinzip vergeben, d.h. die Anwender bekommen nur die Berechtigungen im jeweiligen RSS-IT-System, welche sie für die Umsetzung ihrer Aufgaben benötigen. Der Zugang auf ein RSS-IT-System erfolgt immer über einen Benutzer-Account mit Benutzerkennung und Passwort.

b) Netzwerk

Die Anmeldung erfolgt über einen persönlichen Anmelde-Account. Das dedizierte Passwort muss den Vorgaben der gültigen Passwortrichtlinie entsprechen. IT-System- Administratoren verwenden einen dedizierten, personalisierten Administrator Account für die Arbeiten an Serversystemen. Für Dateien sind differenzierte Zugangsrechte definiert. Die Protokollierung der Zugriffe im Netzwerk erfolgt über einen Log-Eintrag auf den entsprechenden Servern.

c) RSS-Systeme

RSS betreibt neben den von der FLG zur Verfügung gestellten Systeme eigene lokale Systeme. Für die RSS-Systeme sind teilweise separate Accounts notwendig, sofern diese Systeme nicht auf die zentralen (Azure) Active Directory Konten referenzieren (SSO). Systemabhängig gelten die Ausführungen aus Ziff. 3. Schnittstellen zwischen RSS IT Systemen verwenden einen System-Account und sind mit einem Passwortschutz versehen. Zudem erfolgt der Datenaustausch über die externen Schnittstellen verschlüsselt (SSL bzw. IPSec). Webservice-Schnittstellen werden zudem über separate FLG- bzw. RSS-Zertifikate gesichert, wobei die Zertifikatsprüfung bei jeder Transaktion (Zugriff) erfolgt.

d) FLG-Systeme

Für die FLG-Systeme, die von RSS genutzt werden, sind FLG-Accounts notwendig. Nur mit diesen FLG-Accounts kann auf die FLG-Systeme durch RSS-Mitarbeiter zugegriffen werden. Systemabhängig gelten die Ausführungen aus Ziff. 3. Schnittstellen zwischen RSS und FLG-IT-Systemen verwenden einen System-Account und sind mit einem Passwortschutz belegt. Zudem erfolgt der Datenaustausch über die Schnittstellen verschlüsselt (SSL bzw. IPSec). Webservice-Schnittstellen werden zudem über separate FLG- bzw. RSS-Zertifikate gesichert, wobei die Zertifikatsprüfung bei jeder Transaktion (Zugriff) erfolgt.

e) Kundensysteme

Es gibt einzelne Anwendungsfälle im Kundensupport und in der Beratung, bei denen die RSS oder eines ihrer verbundenen Unternehmen Zugriff auf Kundensysteme durch ihre Mitarbeiter notwendig macht. In solchen Fällen werden selbstverständlich die notwendigen Dokumente (z.B. Vertraulichkeitsvereinbarungen) im Vorfeld abgeschlossen. Diese Zugriffe erfordern eine

Authentifizierung seitens der RSS- Mitarbeiter als auch ggf. spezielle Software, Hardware, Zertifikate und Tokens. Zudem muss die RSS sicherstellen, dass nur die benannten Mitarbeiter Zugang zu den kundenspezifischen Zugangsdaten und Geräten haben.

2.4 Vernichtung von Daten

Die Maßnahmen zur Datenlöschung sind in das Löschkonzept der RSS (vgl. Ziff. 7) mit einbezogen. Zur Löschung von Daten sind darin Löschregeln definiert. Zudem ist gewährleistet, dass außerordentliche Löschaufträge (z.B. Löschverlangen einer betroffenen Person) unverzüglich umgesetzt werden können.

Vertrauliche Daten auf Papier oder elektronischen Datenträgern wie Festplatten oder auch Backupbänder werden über spezielle Fachfirmen nach aktuellem Stand der Technik, fachgerecht vernichtet. Zusätzlich werden alle Datenträger vor Weitergabe nach einem sicheren Verfahren mehrfach mit Zufallswerten überschrieben.

Das Löschkonzept sieht Maßnahmen zur Protokollierung der Datenlöschung und zum Umgang mit Sondersituationen (z.B. Löschung scheitert) vor. Die Bestätigung über den Löschvorgang können dabei einem Auftraggeber der RSS auf Anfrage in elektronischer Form zur Verfügung gestellt werden.

Eine Vernichtung (Löschung) von Daten in Public-Cloud Systemen (Office365, Azure) ist über den Hostingvertrag vereinbart, so dass die RSS-IT-System-Administratoren diese Datenlöschung beauftragen und kontrollieren können.

2.5 Trennungsgebot

Die RSS hat Maßnahmen ergriffen, um zu gewährleisten, dass personenbezogene Daten, die zu unterschiedlichen Zwecken oder für unterschiedliche Verantwortliche bzw. Auftraggeber erhoben wurden, getrennt verarbeitet und genutzt werden (sog. Mandantenfähigkeit).

- Trennung von Produktiv- und Testsystemen
- getrennte Ordnerstrukturen (Auftragsverarbeitung)
- separate Tabellen innerhalb von Datenbanken
- getrennte Datenbanken

Alle RSS-Mitarbeiter sind angewiesen und geschult, personenbezogene Daten nur im Rahmen der Dienstleistungserbringung und unter Wahrung der Zweckbindung zu erheben, zu verarbeiten oder zu nutzen. Personenbezogene Daten von Auftraggebern (z.B. Kunden) werden nur im Rahmen des Vertrags, zu dessen Erfüllung genutzt.
In allen wichtigen Bereichen ist das Prinzip der Funktionstrennung eingeführt. Damit sind alle in die Datenverarbeitung eingebundenen Fachbereiche organisatorisch, funktionell und auch räumlich voneinander getrennt.

In den RSS-IT-Systemen werden personenbezogen Daten der Kunden bzw. Mitarbeiter über separate Metadaten bzw. Datensätze (logische Trennung) verwaltet. Zudem erfolgt eine Trennung von Test- und Produktivsystemen. In den Testsystemen sind keine „realen“ personenbezogenen Daten enthalten und werden nur zu Testzwecken mit fiktivem Inhalt angelegt. Diese Trennung bezieht sich auch auf die notwendigen Datenbanken der IT-Systeme. Über das RSS-Berechtigungskonzept erfolgt eine Trennung der personenbezogenen Daten in den jeweiligen IT-Systemen auch nach der organisatorischen Zuordnung. Insbesondere sind allgemeine Verschlüsselungsverfahren nach aktuellem Stand der Technik zu berücksichtigen.

Des Weiteren findet auch für sensible Systeme eine Funktionstrennung in Entwicklungs-, Test- und Produktivsystem mit jeweils eigenständigen Datenbanken statt.

2.6 Weitergabe Kontrolle

Die RSS stellt durch ihre TOMs sicher, dass personenbezogene Daten bei der elektronischen Übertragung oder beim Transport oder bei der Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können sowie, dass solche Zugriffe und die Übermittlung dieser Daten innerhalb der RSS-IT- Systemen dokumentiert werden können. Dies umfasst:

- Sicherung bei der elektronischen Übertragung
  - Verschlüsselung
  - VPN
  - Firewall
  - Fax-Protokoll

- Sicherung beim Transport
  - verschlossene Behälter
  - Verschlüsselung

- Sicherung bei der Übermittlung
  - Verfahrensverzeichnis
  - Protokollierungsmaßnahmen

2.7 Weitergabe von Daten an Dritte

Eine Weitergabe von personenbezogenen Daten aus RSS-IT–Systemen findet grundsätzlich nicht statt, möglich ist dies, allerdings sofern nach Maßgabe einer entsprechenden Rechts- bzw. Vertragsgrundlage eine Weitergabe an verbundene Unternehmen, Kunden, Partner oder Lieferanten zulässig ist. Je nach Vertrag mit dem Dritten sind unterschiedliche Daten betroffen. In jedem Fall ist die Weitergabe von Daten durch den Abschluss von Vertraulichkeitsvereinbarungen (nachfolgend „NDA“ genannt) und Auftragsverarbeitungsvereinbarungen (nachfolgend „AV-Vertrag“ genannt) mit dem jeweiligen Dritten abzusichern.

Die Weitergabe erfolgt stets zweckgebunden und über, durch aktuelle Verschlüsselungsmechanismen (SSL oder IPSec) gesicherte, Verbindungen. Näheres ist in einer internen Richtlinie beschrieben und die RSS-Mitarbeiter werden regelmäßig über den Umgang mit personenbezogenen Daten informiert.

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Die RSS hat Maßnahmen zur Eingabekontrolle ergriffen, die gewährleisten, dass nachträglich überprüft werden kann, ob und durch wen personenbezogene Daten eingegeben, verändert oder gelöscht worden sind.
Eine Protokollierung der Eingabe bzw. Änderung personenbezogener Daten erfolgt in den meisten RSS-IT-Systemen durch das System selbst. Bei IT-Systemen ohne automatische Protokollierung des Datenerfassers personenbezogener Daten wird der Erfasser protokollarisch erfasst. Bei RSS-IT-Systemen mit automatischer Protokollierung der Datenerfassung erfolgt die Benutzeridentifikation über den Benutzer- Account.

4. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a i.V.m. 4 Abs. 5 DSGVO)

<u>Ablage von Kundendaten innerhalb der RSS-IT-Systeme</u>

Bei der RSS werden Kundendaten in diversen IT-Systemen gespeichert und verwaltet. Kundendaten dürfen nur nach Maßgabe der hierin beschriebenen Voraussetzungen genutzt und verarbeitet werden. Die RSS betreibt keine Schnittstellen zwischen ihren IT- Systemen und

den IT-Systemen der Kunden, um personenbezogene Daten auszutauschen. Wenn personenbezogene Daten mit Kunden ausgetauscht werden, dann über den Weg der E-Mail oder CryptShare (Verschlüsselungsprogramm/Add-On). In beiden Fällen werden die Daten verschlüsselt übertragen.

5. Verfügbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

5.1 Verfügbarkeitskontrolle

Zum Schutz von Daten gegen Verlust oder zufällige Zerstörung werden verschiedene Arten von Schutzprogrammen (Virenscanner, Firewalls, Spam-Filter, etc.) auf den RSS- Rechnern der RSS-Mitarbeiter als auch auf den Servern in den Serverräumen der RSS bzw. FLG eingesetzt.

Außerdem sind Sicherheitsmaßnahmen (USV, RAID, Monitoring, Brandschutz, Klimatisierung, Backups, Notfallplan) implementiert, um die Verfügbarkeit der Daten sicherzustellen und diese gegen Verlust bzw. Zerstörung zu schützen.

Einige zentrale RSS-Applikationen (CRM, DMS, EPLAN Cloud) sind bei Dienstleistern „gehosted“. Die Dienstleister sind mittels Vereinbarungen zur Auftragsverarbeitung vertraglich auf die Einhaltung der gesetzlichen Anforderungen des Datenschutzes, insbesondere der DSGVO, verpflichtet.

Die jeweiligen Rechenzentren der Dienstleister entsprechen den Verfügbarkeitsanforderungen nach Tier III sowie den geforderten Verfügbarkeitskontrollen nach DSGVO. Im Kontext des Hosting-Vertrags (AV-Vertrag) sind die Maßnahmen der Verfügbarkeitskontrolle zu prüfen und zu vereinbaren.

5.2 Auftragskontrolle

Die RSS gewährleistet durch mehrere technisch-organisatorische Maßnahmen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, gemäß den Weisungen des Auftraggebers verarbeitet werden. Dies umfasst:

- Festlegung von Weisungsbefugnissen
- Z.B. Darbringung des Nachweises von Zertifizierungen, vor-Ort Kontrollen oder andere hinreichende Garantien (Art. 28 DSGVO)
- Vertrag gemäß den Vorgaben nach Art. 28 DSGVO oder andere geeignete Rechtsinstrumente (z.B. EU-Standardvertragsklauseln)
- Stichprobenprüfung
- Einräumung von Kontrollrechten

Die zur Verarbeitung erhaltenen oder erfassten Daten werden entsprechend den gesetzlichen Vorschriften nur im Rahmen des Auftrages oder der Weisungen des jeweiligen Auftraggebers verarbeitet. Eingesetzte Unterauftragsverarbeiter werden stets durch entsprechende Vereinbarungen schriftlich verpflichtet (z.B. Vertrag über die Auftragsverarbeitung gem. Art. 28 DSGVO, EU-Standardvertragsklauseln oder andere geeignete Maßnahmen).

6. Belastbarkeit der Systeme (Art. 32 Abs. 1 lit. b DSGVO)

Hinsichtlich der Belastbarkeit der Systeme, sieht die RSS insbesondere die nachfolgend aufgeführten Maßnahmen vor:

- Speicher mehr als ausreichend vorhanden und auch kurzfristig jederzeit erweiterbar,

- Systeme und Dienste sind und werden für den nachhaltigen Gebrauch beschafft und genügen den zukünftigen Ansprüchen
- Bandbreite ist für den nachhaltigen Gebrauch beschafft und genügt darüber hinaus zukünftigen Ansprüchen

7. Wiederherstellung von Daten (Art. 32 Abs. 1 lit. c DSGVO)

- Existenz und Aktualisierung eines „Datenwiederherstellungskonzeptes“ für die RSS-
- IT-Systeme
- Backup-Restore-Konzept zur Wiederherstellung verlorener Daten aufgrund von z.B.
- Softwarefehlern, menschlichem Versagen, Hardwaredefekten
- Datensicherungsvorgänge werden überwacht
- Redundante Datenspeicherung
- Redundante IT-Infrastruktur
- Produktive IT-Systeme verfügen über Hot- oder Warm-Standby-Systeme (teilweise in getrennten Rechenzentren abhängig von der Bedeutung der betriebenen Anwendung), um im Fall von Hardwaredefekten, die Verfügbarkeit der jeweiligen Anwendungen zu gewährleisten
- Das Verfügbarkeitskonzept der IT-Systeme wird periodisch auf Funktionsfähigkeit getestet

8. Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

Folgende organisatorische Maßnahmen der RSS gewährleisten, dass die Einhaltung der Anforderungen der DSGVO bzgl. des Schutzes personenbezogener Daten fortlaufend überprüft, bewertet und evaluiert wird:

- Berechtigungskonzepte, Richtlinien und Arbeitsanweisungen zum Umgang mit personenbezogenen Daten (zum Beispiel Datenschutzkonzept) werden regelmäßig überprüft, bewertet und evaluiert;
- das „Datenwiederherstellungskonzept“ für die RSS-IT-Systeme wird regelmäßig überprüft, bewertet und evaluiert;
- der Datenschutzbeauftragte wird regelmäßig fortgebildet;
- regelmäßige Prüfung der technisch-organisatorischen Maßnahmen durch den Datenschutzbeauftragten;
- fortlaufende Überwachung der Auftragsverarbeiter, insbesondere Auswertung der Berichterstattung, einschlägiger Service Levels, und Evaluierung von Änderungsbedarf bzw. konkreter Verbesserungsmaßnahmen
- Die Beschäftigten der RSS werden auf die Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung verpflichtet, deren Grundsätze in Art. 5 Abs. 1 DSGVO festgelegt sind sowie auf sonstige gem.
- zwingender besonderer lokaler und anwendbarer Gesetze existierender Verpflichtungen. Diese Verpflichtungserklärungen erfolgen zur Dokumentierung in schriftlicher Form; im Übrigen erfolgt eine Verpflichtung aller Mitarbeiter auf die Vertraulichkeit.
- kontinuierliche Unterrichtung der RSS-Mitarbeiter durch den Datenschutzbeauftragten bzw. die Fachvorgesetzten nach Anweisung des Datenschutzbeauftragten zur Vertraulichkeit von personenbezogenen Daten
- Rollen- und Funktionsbeschreibungen für die RSS-Mitarbeiter zur Definition der Verantwortlichkeit für bestimmte personenbezogene Daten werden überprüft und angepasst;
- RSS wird regelmäßig durch eine externe Institution über die gesetzeskonforme Umsetzung des Datenschutzes im Unternehmen auditiert
- Im Fall einer Datenverarbeitung im Auftrag werden Auditrechte mit den Auftragsverarbeitern ausgeübt

Die nachfolgenden Dokumente zum Informations-Sicherheits-Management unterliegen einer regelmäßigen (mindestens jährlichen) Überprüfung. Zu diesen Dokumenten zählen u.A:

- Leitlinie zur Informationssicherheit
- Sicherheitsrichtlinie - Informationen und Daten
- Sicherheitsrichtlinie - Betrieb und Support
- Sicherheitsrichtlinie - Systeme (Plattformsicherheit)
- Sicherheitsrichtlinie - Netzwerke

Anlage zu Ziff. 10 - Unterauftragnehmer

Folgende Unterauftragnehmer sind mit Zustimmung des Auftraggebers tätig:

	Name	Kontakt	Vertragspartner Lokation: Unterauftragnehmer
1.	Microsoft Deutschland GmbH	https://azure.microsoft.com/de-de/support/legal/	Deutschland (EU)
2.	Twilio Germany GmbH	https://www.twilio.com/legal/tos	Deutschland (EU)
3.	Hubspot Inc.	https://legal.hubspot.com/legal-stuff	Cambridge (USA)
4.	Google Ireland Ltd.	https://policies.google.com/privacy?hl=de	Irland (EU)
5.	Adobe Systems Software Ireland Ltd.	https://www.adobe.com/de/legal.html	Irland (EU)

EPLAN speichert und verarbeitet die personenbezogenen Daten des Auftraggebers, die im Rahmen der Nutzung der EPLAN Cloud von EPLAN erhoben werden, grundsätzlich DSGVO-konform auf Servern innerhalb des EU-Wirtschaftsraumes.

Die vorgenannten Unterauftragnehmer erbringen folgende Teilleistungen:

	Beschreibung der Teilleistung
zu 1.	Cloud-Hosting-Dienst, Datenspeicherung (Benutzerdatenbank, hochgeladene Dateien)
zu 2.	E-Mail-Versender der automatisierten technischen Mails im Registrierungsprozess (Emailadresse, Nachname)
zu 3.	Analyse zur Optimierung der Benutzererfahrung (Herkunft des Benutzers – Vorherige Seite - Link zur Referenz)
zu 4.	Analyse zur Optimierung der Benutzererfahrung (Browserinformationen: Sprache, Auflösung, installierte Plug Ins, Typ, Zeitzone, Dauer, vorherige Seite)
zu 5.	Content-Management-System, Hosting der Webseite EPLAN.com (Name, Emailadresse, Position)