SanData IT-Gruppe („SanData“)

Vertragsanhang Datenschutz und Datensicherheit

Dieser Vertragsanhang Datenschutz und Datensicherheit nach DSGVO ("Anhang") regelt die Vertraulichkeit und Sicherheit personenbezogener Daten bei SanData im Zusammenhang mit den Services, die im Auftrag des Kunden erbracht werden. Er ist Bestandteil des Vertrags zwischen dem jeweiligen Unternehmen der SanData und dem Kunden, auf dessen Grundlage die Services erbracht werden oder der Allgemeinen Geschäftsbedingungen der SanData IT-Gruppe, falls kein Vertrag besteht ("Vertrag").

1. Dieser Anhang ist Bestandteil des Vertrags und unterliegt dessen Bedingungen. Soweit Widersprüche zwischen den Bedingungen dieses Anhangs und des Vertrags bestehen, hat der Anhang Vorrang.

2. Begriffsbestimmungen (*Art. 4 DSGVO*):

   2.1. "personenbezogene Daten" oder "personenbezogene Kundendaten" bezeichnen (Kunden-) Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (*Art. 4 Nr.1 DSGVO*).

   2.2. "geschäftliche Kontaktdaten" bezeichnet Kontaktinformationen der Vertreter der Kunden zum Zweck der Rechnungsstellung, Abrechnung und sonstiger geschäftlicher Anfragen, (ii) Informationen zur Nutzung der Services durch den Kunden und (iii) sonstige Informationen, die SanData erhebt und benötigt, um mit dem Kunden zu kommunizieren. Diese können zugleich personenbezogene Daten enthalten.

   2.3. "Datenschutzgesetze" bezeichnet alle geltenden Gesetze und Vorschriften in Bezug auf die Verarbeitung von personenbezogenen Daten und Datenschutz, die in den jeweiligen Rechtsordnungen bestehen können. Insbesondere die Verordnung (EU) 2016/679 (DSGVO) sowie das Bundesdatenschutzgesetz (BDSG n.F.).

   2.4. "Verantwortlicher" bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die nach geltendem Datenschutzrecht allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (*Art. 4 Nr. 7 DSGVO*).

   2.5. "Auftragsverarbeiter" bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogenen Daten im Auftrag des Verantwortlichen oder auf Weisung eines anderen Auftragsverarbeiters, der im Auftrag des Verantwortlichen handelt, verarbeitet (*Art. 4 Nr. 8 DSGVO*).

   2.6. "verarbeiten", "Verarbeitung" oder "verarbeitet" bezeichnet jeden mit oder ohne Zuhilfenahme automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten (einschließlich Zugriff, Erheben, Erfassen, Organisation, Aufbewahrung, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung, Bereitstellung, Abgleich, Verknüpfung, Sperren, Löschen oder Vernichtung von personenbezogenen Daten) und entsprechende Begriffsbestimmungen in einschlägigen Datenschutzgesetzen, soweit eine solche diese Definition ändern sollte (*Art 4 Nr. 2 DSGVO*).

3. Rechte und Pflichten sowie Weisungsbefugnisse des Kunden (*Art. 28 Abs. 3 lit. a DSGVO*):

   3.1. SanData verarbeitet personenbezogene Kundendaten in dem Umfang, der für die Erbringung der Services und die Erfüllung der Pflichten von SanData im Rahmen dieses Anhangs, des Vertrags und der anwendbaren Datenschutzgesetze als (Unter-)Auftragsverarbeiter von personenbezogenen Kundendaten erforderlich ist. Einzelheiten der Verarbeitung, einschließlich Gegenstand, Zweck und Dauer der Verarbeitung, Arten personenbezogener Daten und Kategorien personenbezogener Daten, auf die sich die Daten beziehen, sind in Anlage A aufgeführt (*Art. 28 Abs. 3 DSGVO*).

   3.2. SanData verarbeitet personenbezogene Kundendaten gemäß den in diesem Anhang aufgeführten Anweisungen des Kunden, dem Vertrag oder sonstigen dokumentierten Anweisungen zwischen SanData und dem Kunden. Mögliche Kosten und Gebühren im Zusammenhang mit diesen zusätzlichen Anweisungen sind gemäß den Bedingungen des Vertrags zu vereinbaren. SanData darf personenbezogene Kundendaten auf andere Weise als gemäß den Anweisungen des Kunden verarbeiten, sofern SanData hierzu gesetzlich verpflichtet ist. In diesem Fall informiert SanData den Kunden von diesem Erfordernis, bevor SanData personenbezogene Kundendaten verarbeitet, sofern dies nicht gesetzlich aus wichtigen Gründen des öffentlichen Interesses untersagt ist. Ist SanData nicht in der Lage, aufgrund von Gesetzen oder Gesetzesänderungen die Anweisungen des Kunden oder diesen Anhang einzuhalten, bzw. sofern SanData der Auffassung ist, dass eine Anweisung des Kunden geltendes Recht verletzt oder sofern ein sonstiger Grund vorliegt, informiert SanData den Kunden unverzüglich schriftlich Nutzt der Kunde die Services, um Kategorien von Daten zu verarbeiten bzw. durch SanData im Auftrag verarbeiten zu lassen, die nicht ausdrücklich von diesem Anhang umfasst sind, handelt der Kunde auf eigenes Risiko (*Art. 28 Abs. 3 lit. a DSGVO*).

   3.3. Die SanData gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (*Art. 28 Abs. 3 lit. b DSGVO*).

4. Einhaltung von Gesetzen

4.1. Die Parteien kommen zu jedem Zeitpunkt ihren jeweiligen Pflichten im Rahmen dieses Anhangs und der einschlägigen Datenschutzgesetze nach, die für ihre jeweilige Verarbeitung personenbezogener Daten gelten.

4.2. SanData hält außerdem sämtliche einschlägigen Gesetze und die Datenschutzrichtlinie von SanData in Bezug auf die Verarbeitung geschäftlicher Kontaktdaten ein und verwendet geschäftliche Kontaktdaten ausschließlich für berechtigte geschäftliche Zwecke, einschließlich Rechnungsstellung, Beitreibung, Überwachung und Optimierung der Service-Nutzung, Service-Verbesserungen, Wartung, Support, Mitteilungen bezüglich Vertragsverlängerungen zu Zwecken der Vertragsverlängerung direkt oder über einen Unterauftragsverarbeiter, der im Auftrag von SanData handelt und Informationen über neue und weitere Services.

4.3. Legt SanData oder seine Mitarbeiter selbst personenbezogene Daten von SanData Mitarbeitern (einschließlich personenbezogener Daten der Mitarbeiter von mit SanData verbundenen Unternehmen, Unterauftragnehmern, Partnern und Kunden von SanData) gegenüber Kunden offen bzw. dem Kunden zur Verfügung, die der Kunde verarbeitet, um seine Nutzung der Services zu verwalten, so verarbeitet der Kunde diese Daten gemäß seinen Datenschutzrichtlinien und den geltenden Datenschutzgesetzen. Eine solche Offenlegung durch SanData erfolgt nur, sofern sie für die Zwecke des Vertrags-Managements, Service-Managements oder zu den Zwecken einer angemessenen und rechtmäßigen Hintergrundprüfung durch den Kunden oder Sicherheitszwecken rechtmäßig ist.

5. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (*Art. 28 Abs. 3 Satz 2 lit. c DSGVO*)

5.1. SanData implementiert und führt die in Anlage B aufgeführten physischen, technischen und organisatorischen Maßnahmen durch, um die personenbezogenen Kundendaten und geschäftlichen Kontaktdaten vor unbeabsichtigter oder unrechtmäßiger Vernichtung oder unbeabsichtigtem Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugriff zu schützen.

5.2. Der Kunde erkennt an, dass SanData die Sicherheitsmaßnahmen durch die Einführung neuer oder verbesserter Sicherheitstechnologien verändern kann, und gestattet SanData, diese Änderungen vorzunehmen, sofern sie das Schutzniveau nicht mindern. SanData stellt auf Verlangen dem Kunden Informationen über die aktuellsten, auf die Services anwendbaren Maßnahmen zur Datensicherheit zur Verfügung.

6. Unterauftragsverhältnisse mit Subunternehmern (*Art. 28 Abs. 3 Satz 2 lit. d DS-GVO*)

6.1. Der Kunde gestattet SanData, verbundene und nicht verbundene Unterauftragsverarbeiter von SanData ("Unterauftragsverarbeiter") zu beauftragen, die einige oder alle der vertraglichen Pflichten von SanData erfüllen. SanData gewährt seinen Unterauftragsverarbeitern nur insoweit Zugang zu personenbezogenen Kundendaten, wie dies für die Erbringung der Services erforderlich ist.

6.2. Die Unterauftragsverarbeiter, die für die Services eingesetzt werden können, und die Orte der Verarbeitung können in Anlage C eingesehen werden. Etwaige auftragsspezifische Unterauftragsverarbeiter sind in diesem Anhang ebenfalls in Anlage C aufgeführt. Die entsprechenden Unterauftragsverarbeiter gelten als vom Kunden genehmigt. Die SanData informiert den Kunden immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters, wodurch der Kunde die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Die Parteien unternehmen alle zumutbaren Anstrengungen, um auf den Widerspruch des Kunden hin eine einvernehmliche Lösung zu finden. Gelingt dies nicht innerhalb einer angemessenen Zeit, sind die Parteien berechtigt, den Vertrag ohne weitere Verpflichtungen zu kündigen.

6.3. SanData prüft seine Unterauftragsverarbeiter sorgfältig und schließt mit den Unterauftragsverarbeitern wirksame, durchsetzbare Verträge, nach denen die Unterauftragsverarbeiter verpflichtet sind, Bedingungen einzuhalten, die in Bezug auf die Verarbeitung und den Schutz personenbezogener Kundendaten mindestens den Schutz vorsehen wie die Bedingungen dieses Anhangs (einschließlich der EU-Standardvertragsklauseln in Bezug auf Datenimporteure im Fall einer Weiterübermittlung von personenbezogenen Daten aus der EU, dem EWR oder der Schweiz in ein Drittland ohne angemessenes Schutzniveau).

6.4. SanData haftet für Handlungen und Unterlassungen der von ihm mit der Erbringung der Services für die Kunden beauftragten Unterauftragsverarbeiter, die einen Verstoß gegen diesen Anhang darstellen, wie für eigene Handlungen oder Unterlassungen (*Art. 28 Abs. 4 DSGVO*).

7. Prüfungen, Inspektionen und Kontrollrechte durch den Kunden (*Art. 28 Abs. 3 lit. h DSGVO*)

7.1. SanData veranlasst interne und externe Prüfungen der Datenverarbeitungs- und Datenschutzmaßnahmen von SanData, um die Einhaltung geltender Datenschutzgesetze sicherzustellen und überlässt auf Verlangen des Kunden einen zusammenfassenden Bericht und weitere Informationen.

7.2. Der Kunde hat das Recht, gemäß Vertrag zusätzliche Prüfungen durchzuführen, ob SanData seine Pflichten im Rahmen dieses Anhangs einhält. Die Prüfungsrechte werden im Allgemeinen in Absprache mit SanData zu Geschäftszeiten ausgeübt. SanData ist verpflichtet, den Kunden oder die zuständige Datenschutzbehörde bei diesen Prüfungen zu unterstützen. Die Prüfungen sind unter Berücksichtigung der Betriebsabläufe und der für SanData erforderlichen Sicherheit und Vertraulichkeit durchzuführen.

7.3. Bei bestimmten Informationen zu den Sicherheitsmaßnahmen und -praktiken bei SanData handelt es sich um sensible vertrauliche Informationen, die von SanData gegenüber dem Kunden nicht offengelegt werden. SanData erklärt sich damit einverstanden, auf Verlangen nicht mehr als einmal pro Jahr einen angemessenen Fragebogen zur Informationssicherheit in Bezug auf die für die im Rahmen dieses Anhangs erbrachten Services spezifischen Sicherheitspraktiken zu beantworten.

7.4. Auf Verlangen des Kunden stellt SanData innerhalb angemessener Zeit dem Kunden Informationen in angemessenem Umfang zu Verfügung, um die Einhaltung der geltenden Datenschutzgesetze nachzuweisen, sofern nicht diese Informationen dem Kunden direkt durch die Nutzung der Services ohne weiteres zugänglich sind.

8. Dem Kunden gewährte Unterstützung (*Art. 28 Abs. 3 lit. f DSGVO*)

8.1. Auf Verlangen des Kunden arbeitet SanData mit dem Kunden zusammen und gewährt ihm diejenige Unterstützung, die erforderlich ist, um die Verarbeitung der personenbezogenen Kundendaten gemäß den für den Kunden geltenden Datenschutzgesetzen in Bezug auf die SanData Services zu ermöglichen, beispielsweise durch:

8.1.1. Unterstützung des Kunden bei der Implementierung angemessener technischer und organisatorischer Maßnahmen, soweit dies möglich ist sowie angemessene Unterstützung des Kunden bei seiner Pflicht, auf Anträge natürlicher Personen zu reagieren, die ihre Rechte gemäß der für den Kunden geltenden Datenschutzgesetze ausüben möchten (*Art. 28 Abs. 3 lit. e DSGVO*);

8.1.2. angemessene Unterstützung des Kunden bei der Beurteilung und Implementierung angemessener technischer und organisatorischer Maßnahmen, um ein Datenschutzniveau herzustellen, das für die mit der Datenverarbeitung verbundenen Risiken und die Art der personenbezogenen Kundendaten angemessen ist;

8.1.3. Meldung von Sicherheitsvorfällen gemäß Anlage A;

8.1.4. angemessene Unterstützung des Kunden bei der Durchführung einer Datenschutz-Folgenabschätzung.

8.2. Verlangt der Kunde Zusammenarbeit oder Unterstützung gemäß dieser Klausel, so hat er SanData die Anforderungen und Anweisungen schriftlich mitzuteilen. SanData reagiert innerhalb einer angemessenen Frist und lässt dem Kunden eine ungefähre Zeit- und Kostenschätzung für die Implementierung der Änderungen zukommen, die erforderlich sind, um die Compliance-Anforderungen des Kunden umzusetzen. Soweit die Einhaltung dieser Klausel eine Änderung des Umfangs der Services bedeutet, werden die Parteien in angemessener Weise einen entsprechenden Änderungsauftrag vereinbaren.

9. Verpflichtungen der SanData während und nach Beendigung des Auftrags (*Art. 28 Abs. 3 Satz 2 lit. g DS-GVO*)

9.1. Soweit es dem Kunden nicht selbst möglich ist, auf personenbezogene Kundendaten zuzugreifen, wird SanData auf schriftliches Verlangen des Kunden (i) personenbezogene Kundendaten aktualisieren, berichtigen oder löschen und/oder (ii) Kopien der personenbezogenen Kundendaten zur Verfügung stellen.

9.2. Bei Beendigung des Vertrags gibt SanData nach Wahl des Kunden die personenbezogenen Kundendaten zurück oder löscht sie. SanData behält keine Kopien der personenbezogenen Kundendaten zurück, sofern nicht mit dem Kunden etwas anderes vereinbart ist oder SanData nach geltendem Recht dazu verpflichtet ist; in diesem Fall stellt SanData die aktive Verarbeitung der Daten ein und wahrt die Sicherheit und Vertraulichkeit der Daten.

9.3. In Bezug auf die Reparatur oder den Austausch von Datenträgern (Servern, Festplatten, SSD, Flash-Disks, Speichern etc.) kauft der Kunde entweder den optionalen Service oder löscht die Datenträger bzw. die sich darauf befindlichen Daten ausreichend, bevor er sie SanData überlässt.

10. Datenübermittlungen in Drittstaaten

10.1. Eine Beauftragung von Subunternehmern in Drittstaaten erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

10.2. Um die Übermittlung von personenbezogenen Daten aus der EU, dem EWR oder der Schweiz durch den Kunden oder ein mit dem Kunden verbundenes Unternehmen an SanData oder ein mit SanData verbundenes oder nicht verbundenes Unternehmen, das in einem Land ansässig ist, dem von der Europäischen Kommission kein hinreichender Schutz personenbezogener Daten gemäß Artikel 25 Abs. 6 der Richtlinie 95/46/EG oder Artikel 45 Abs. 3 der Datenschutzgrundverordnung bestätigt wurde, zu regeln, ist im Zusammenhang mit den Services ein EU-Auftragsdatenverarbeitungsmustervertrag ("EU-Standardvertragsklausel") zu schließen. Der Kunde genehmigt SanData hiermit, in seinem Namen und im Namen seiner verbundenen Unternehmen einen EUMustervertrag abzuschließen.

11. Haftung

11.1. Sofern keine andere vertragliche Haftungsvereinbarung vorliegt, gelten für alle gesetzlichen und vertraglichen Schadens- und Aufwendungsersatzansprüche des Kunden folgende Regelungen:

11.2. Bei leicht fahrlässigen Pflichtverletzungen wird die Haftung grundsätzlich auf den Auftragswert beschränkt. Beträgt der Auftragswert weniger als 50.000,- €, wird die Haftung auf 50.000,- € beschränkt. Im Falle von Sachschäden ist die Haftung auf eine Million Euro beschränkt, wenn der Auftragswert geringer als eine Million Euro ist.

11.3. Bei Verlust von Daten haftet die SanData nur für denjenigen Aufwand, der bei ordnungsgemäßer und regelmäßiger Datensicherung durch den Kunden für die Wiederherstellung der Daten erforderlich gewesen wäre. Die Beschränkung gilt nicht, wenn und soweit die Datensicherung Bestandteil der von SanData zu erbringenden Leistungen ist.

11.4. Ansprüche aus entgangenem Gewinn sind ausgeschlossen, soweit nichts anderes vereinbart ist.

11.5. Die Haftungsbeschränkungen gelten nicht für Ansprüche wegen Vorsatz und grober Fahrlässigkeit, bei der Verletzung des Lebens, des Körpers oder der Gesundheit, bei Arglist, soweit das Produkthaftungsgesetz zur Anwendung kommt, sowie bei Garantieversprechen, soweit bzgl. letzteren nichts anderes geregelt ist.

12. Schlussbestimmungen

12.1. Sollten die Daten des Kunden beim der SanData durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat die SanData den Kunden unverzüglich darüber zu informieren. Die SanData wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Kunden als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

12.2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen der SanData – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

12.3. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

12.4. Es gilt deutsches Recht.

Anlage A - Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

SanData nimmt im Rahmen der Leistungserbringung die folgende Verarbeitung personenbezogener Daten vor	Im Rahmen der Erbringung von Leistungen zur Hardware- und Software-Wartung vor Ort und per Fernzugriff (Remote) sowie bei (Komplettsystem-)Installationen hat SanData möglicherweise Zugang zu Daten, die in den Geschäftsanwendungen, der IT und Netzwerk-Infrastruktur des Kunden gespeichert sind. Wobei nicht auszuschließen ist, dass diese Daten personenbezogene Daten enthalten.

Art der verarbeiten personenbezogenen Kundendaten	Die Art der verarbeiteten personenbezogenen Daten hängt von den Daten ab, die der Kunde in den Geschäftsanwendungen, der IT und Netzwerkinfrastruktur gespeichert ab, und kann besondere Kategorien personenbezogene Daten umfassen.

Kategorien betroffener Personen	Jede betroffene Person, deren personenbezogene Daten vom Kunden in den Geschäftsanwendungen, der IT und Netzwerk-Infrastruktur gespeichert werden, einschließlich Kunden des Kunden, Endnutzern, Mitarbeitern, (Unter-)Auftragnehmern und Leiharbeitnehmern.

Dauer der Verarbeitung	SanData verarbeitet die personenbezogenen Kundendaten soweit dies im Rahmen des Vertragsverhältnisses sowie gesetzlicher Vorgaben (Bspw. Abgabenordnung) erforderlich und zulässig ist.

Anlage B - Beschreibung der vom Auftragnehmer zum Schutz der Daten des Auftraggebers getroffenen technischen und organisatorischen Maßnahmen („TOMs“)

GESETZLICHE VORGABE			DETAILLIERTE BESCHREIBUNG DER VOM AN GETROFFENEN SICHERHEITSMASSNAHMEN
1.	**Zutrittskontrolle**	**Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.**	**Alle Räumlichkeiten der SanData EDV-Systemhaus GmbH sind zutrittsbeschränkt. Zutritt via Firmenschlüssel erhalten Mitarbeiter des jeweiligen Standorts, wobei eine Eintragung dieser Mitarbeiter mit Firmenschlüssel in das Schlüsselbuch namentlich und mit Schlüsselnummer erfolgt.** **Besuchern wird der Zutritt nur nach Voranmeldung (elektrische Türöffner mit Gegensprechanlage und Kamera) gestattet. Besucher werden während ihres gesamten Aufenthalts in den Räumlichkeiten durch SanData Mitarbeiter begleitet.**
2.	**Zugangskontrolle**	**Es ist zu verhindern, dass Datenverarbeitungssysteme von Unb genutzt werden können.**	**Alle Arbeitsstationen sind durch personenbezogene Zugangsdaten geschützt (Benutzername + Passwort).** **Die Passwortsyntax hat einen hohen Schutz (Länge mind. 9 Zeichen, Mix aus Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen). Passwörter müssen alle 90 Tage erneuert werden, wobei ein Abgleich mit den letzten 5 vergebenen Passwörtern stattfindet. Nach 15 Minuten Inaktivität findet eine automatische Sperrung der Clients statt die nur durch Eingabe des Passwortes aufgehoben werden kann.** **Der externe Zugang der Mitarbeiter auf das LAN und die Firmenlaufwerke ist nur per SSL-VPN Verbindung möglich. Die Zugangsdaten werden hier durch einen RSA-Token (2048 Bit Schlüssel einer selbst erstellten digitalen Signatur sowie Benutzername) erzeugt.** **Dies ist eine 2Faktoren-Authentifizierung bei der es sich um ein einmal Passwort handelt. Dies wird mit einer festen 4stelligen Pin und einer alle 60 Sekunden, einmalig neu erzeugter Tan, erstellt.** **Firmeneigene Notebooks werden mittels Zertifikat und Benutzerkennung automatisch über den Microsoft Dienst „Direct Access“ mit dem Firmennetz verbunden.** **Die Sperrung eines Zugangs erfolgt in allen Fällen nach 5maliger falscher Anmeldung.** **Alle Datenträger (Festplatten) der Notebooks sind mittels BitLocker AES 256Bit verschlüsselt.**

3.	**Zugriffskontrolle**	**Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.**	**Allen Mitarbeitern werden dediziert Zugriffsberechtigungen vergeben. Die technische Umsetzung erfolgt per Microsoft Berechtigungskonzept mit differenzierten Berechtigungen und Protokollierungen der Zugriffe. Das heißt, die Mitarbeiter werden je nach Einsatz- und Tätigkeitsbereich den Benutzergruppen in der AD mit Ihrem erstellten Profil zugeordnet. Sensible Daten die auf verschlüsselte Laufwerken liegen, erfordern eine gesonderte Anmeldung mittels digitaler Signatur.** **Als Kontrollmaßnahme finden regelmäßige interne Prüfläufe (administrative Überprüfung des Berechtigungskonzeptes und der AD) der Berechtigungsvergaben statt.** **Ausgeschiedene Mitarbeiter werden vom System entfernt. Dies ist durch Prozesse und organisatorisch geregelt.**

4.	**Weitergabekontrolle**	**Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.**	**Die elektronische Übertragung erfolgt unter Verwendung von VPN-und SSL Verschlüsslungen (256Bit AES Schlüssel) inklusive deren Protokollierung** **(Logdateien auf der Firewall) im Rahmen des BDSG n.F.. Firewall Systeme und ständig aktualisierte Virensoftware sichern neben einer Secure Socket Layer (SSL mit 256Bit AES) Verschlüsselung und dem Einsatz von VPNTechnologien (IPsec SHA1 AES 256Bit preshared Key) die Kommunikation via Internet. Bei Fernzugriffen erfolgt die Userauthentifizierung mittels RSA (2048Bit Schlüssel) einer digitalen Signatur und Benutzernamen. Laufwerke mit besonders sensiblen Daten werden unter Einsatz eines Zertifikates verschlüsselt. Notebook-Festplatten werden generell mit BitLocker verschlüsselt.** **Es werden nur Datenträger die in Notebooks verbaut sind transportiert. Diese sind mit BitLocker verschlüsselt.** **E-Mails können bei Bedarf verschlüsselt versendet werden. Innerhalb der IT-Gruppe können E-Mails per S-MIME verschlüsselt werden.** **SPX-Verschlüsselung kann bei externem E-Mail-Versand erfolgen.**
5.	**Eingabekontrolle**	**Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.**	**Aufzeichnung des Protokolls unmittelbar mit dem betreffenden Datensatz und Speicherung der dazugehörigen Log-Dateien.** **Eine regelmäßige Auswertung findet nicht statt.** **Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts.**

6.	**Auftragskontrolle**	**Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.**	**Dies erfolgt unter Verwendung von Formularen, Merkblättern und Arbeitsanweisungen um eine korrekte Auftragsverarbeitung sicherzustellen.** **Diese Dokumente sind im Intranet der SanData IT-Gruppe hinterlegt und für jeden Mitarbeiter zugänglich.** **Einweisung und wiederkehrende Schulungen der Mitarbeiter in die entsprechenden Vorschriften und Anweisungen. Dokumentation per elektronisch dokumentiertem Schulungsnachweis.** **Eine eindeutige Vertragsgestaltung (Auftragsverarbeitungsvertrag) sowie eine formalisierte Auftragserteilung (Auftragsformular) erfolgt durch den Auftraggeber. Beim Einsatz von Subunternehmern werden die gesetzlichen Vorgaben (AVV, Geheimhaltungsverpflichtung, Kontrollmaßnahmen) eingehalten und Umgesetzt.**
7.	**Verfügbarkeitskontrolle**	**Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.**	**Backupkonzept inkl. Rücksicherungstests, Auslagerung der Sicherungs-bänder außerhalb des Firmengebäudes.** **Ein Backup-Plan liegt vor. Einmal wöchentlich wird ein Backupprotokoll erstellt das dem IT-Sicherheitsbeauftragten zur Kontrolle übergeben wird. Regelmäßige Rücksicherungsläufe finden statt.** **Verantwortlichkeiten für den täglichen Betrieb sowie für den Notfall sind organisatorisch geregelt.** **Technische Mittel:** **USV-Anlage, Backupsysteme, Serverräume außerhalb von Gefährdungsbereichen. Raid- und Storage Systeme, Firewalls, Content Security Systeme, mehrfach gestaffeltes Virenschutzkonzept. Relevante Daten werden verschlüsselt mit Veeam Backup & Replication gesichert.**
8.	**Trennungskontrolle**	**Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.**	**Die Trennung der Daten erfolgt rollenbasierend unter Einbeziehung des Berechtigungskonzeptes. Daten können nur von Authentifizierten und zugriffsberechtigten Mitarbeitern nach Vorgabe des Auftraggebers verarbeitet werden. Strikte Trennung von Produktiv und Testdaten in getrennten, virtuellen Umgebungen.**
9.	**IT-Sicherheitsanalyse im Rahmen der** **DS-GVO** **(Datenschutz-Grundverordnung / Verordnung EU 2016/679)**	**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.**	**Mittels eines kontinuierlicheren Prozesses werden die Systeme der SanData IT-Gruppe überwacht und permanent auf den Stand der Technik gehalten.** **Um dies zu dokumentieren, findet jährlich eine IT-Sicherheitsanalyse im Rahmen der DS-GVO** **(Datenschutz-Grundverordnung / Verordnung EU 2016/679) durch eine externes IT-Sicherheits-Unternehmen** **statt.**
10.	**Pseudonymisierung**	**Eine Pseudonymisierung findet nicht statt.**	

Stand: 11.12.2019

Anlage C - Liste der genehmigten Subunternehmer

I. “Unternehmen der SanData IT-Gruppe”

Gesellschaft	Anschrift
SanData IT-Trainingszentrum GmbH	Emmericher Str. 17, DE-90411 Nürnberg
SanData EDV-Systemhaus GmbH	Emmericher Str. 17, DE-90411 Nürnberg
ProTeam Business Solutions GmbH	Lise-Meitner-Straße 14, DE-74074 Heilbronn
SanData Solutions GmbH	Emmericher Str. 17, DE-90411 Nürnberg
SanData Technology GmbH & Co. KG	Amalienstraße 65, AT-1130 Wien
CCC City Computer Contor GmbH	Emmericher Str. 17, DE-90411 Nürnberg
Data Technology Betriebsberatungs GmbH & Co. KG	Amalienstraße 65, AT-1130 Wien

II. Weitere auftragsspezifische Unterauftragsverarbeiter (sofern einschlägig):

Gesellschaft	Anschrift	Erbrachte Leistung

DATUM UND UNTERSCHRIFT	DATUM UND UNTERSCHRIFT
NAME DES KUNDEN	SanData UNTERNEHMEN ("SanData")
EINGETRAGENE ANSCHRIFT	EINGETRAGENE ANSCHRIFT
NAME DES UNTERZEICHNERS	NAME DES UNTERZEICHNERS
POSITION	POSITION