# Zusätzliche Vertragsbedingungen zur Einhaltung des Datenschutzes und Wahrung von Geschäftsgeheimnissen am Klinikum Nürnberg (DVB-Kh)

**- Bewerbungs- und Vertrags-Bedingungen -** - Ausgabe Januar 2019 -

**1. Rechtsgrundlagen und Vertragsbestandteile**

Diese Vertragsbedingungen finden Anwendung auf Verträge und vorvertragliche Verhandlungen zwischen dem Klinikum Nürnberg und den mit diesem verbundenen Unternehmen - im folgenden Auftraggeber genannt - und Unternehmen, Einzelkaufleuten, freiberuflich tätigen Selbständigen, etc - im folgenden Auftragnehmer genannt-, die im Auftrag des Klinikums Nürnberg bzw. den mit diesen verbundenen Unternehmen freiberufliche Dienst- und Werkvertragsleistungen, Leistungen nach der Verordnung über die Vergabe öffentlicher Aufträge (VgG), Bauleistungen nach der Vergabe- und Vertragsordnung für Bauleistungen (VOB), oder andere Leistungen oder Lieferungen nach BGB und HGB sowie Vertragsverhandlungen oder – Vorverhandlungen nach der Vergabe- und Vertragsordnung für Leistungen (VOL) oder Leistungen und Lieferungen nach der Unterschwellenvergabeordnung (UVgO) erbringen bzw führen. Die Vertragsbedingungen gelten auch für Subunternehmer und Unternehmen, die im Auftrag des Auftragnehmers tätig werden. Umfasst der Auftrag Lieferung, Wartung, Miete, Reparatur oder anderweitige Betreuung von informationsverarbeitenden Systemen oder med.-techn. Geräten des Auftraggebers, so gelten zusätzlich zu Punkt 2 die Ausführungen unter Punkt 3. (Datenschutzbedingungen bei Wartung und Fernwartung), 4 und 5 (Leihe).

**Rechtsgrundlagen sind:**

- Die DSGVO, das BayDG, und das Bundesdatenschutzgesetz (BDSG)
- Artikel 27 des Bayerischen Krankenhausgesetzes
- weitere einschlägige Bestimmungen aus dem Bürgerlichen Gesetzbuch, dem Straf- und dem Urheberrecht

**2. Verpflichtung zur Verschwiegenheit**

2.1 Der Auftragnehmer verpflichtet, sich über alle im Rahmen seiner Tätigkeit oder bei Gelegenheit der Auftragserfüllung erlangten Kenntnisse von personenbezogenen Daten des Auftraggebers oder von Daten, die unter das Geschäftsgeheimnis des Auftraggebers oder von Daten die unter Berufsgeheimnisse von beim Auftraggeber tätigen Personen fallen, Stillschweigen zu bewahren, nicht unbefugt zu offenbaren, diese Daten nicht für andere als vertraglich festgelegte Zwecke zu verwenden oder unbeteiligten Dritten weiterzugeben. Der Auftraggeber weist den Auftragnehmer ausdrücklich auf die mögliche Strafbarkeit nach §§ 203 Abs. 4, 204 StGB hin.
Diese Verpflichtung besteht auch über das Ende des Auftrags fort.

2.2 Der Auftragnehmer verpflichtet sich, seine Mitarbeiter, Erfüllungsgehilfen und Unternehmen, die für ihn im Auftrag tätig sind, auf Einhaltung der unter Punkt 2.1 genannten Pflichten in Textform zu verpflichten. Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.
Der Auftragnehmer hat seine Mitarbeiter, auch für die Zeit nach Beendigung dieses Auftrages oder nach Beendigung der Mitarbeit zu verpflichten.

**3. Datenschutz und -sicherheit bei Wartung und Fernwartung informationsverarbeitender Systeme, einschließlich medizinisch-technischer Systeme**

**3.1 Wartung**

3.1.1 Der Auftragnehmer verpflichtet sich, im Rahmen von Wartungsarbeiten, den Zugang zu Netzwerken, Computern, Programmsystemen und zu medizinisch-technischen Geräten ausschließlich zu dem vertraglich festgelegten Zweck zu verwenden.

3.1.2 Der Auftragnehmer muß nachweisen können, wann welche seiner Mitarbeiter zur Wartung an Systemen des Auftraggebers eingesetzt wurden. Soweit das Wartungspersonal dem Auftraggeber nicht bekannt ist, muß es sich als solches ausweisen können.

3.1.3 Der Zugang zu Rechnersystemen des Auftraggebers darf nur unter den Sicherheitsvorkehrungen und -bedingungen des Auftraggebers erfolgen. Insbesondere werden notwendige Benutzerberechtigungen, Passworte und Zugriffsrechte ausschließlich vom Auftraggeber erteilt.

3.1.4 Der Auftragnehmer verpflichtet sich, ausschließlich Personal mit der Wartung zu betrauen, das gemäß den Vorgaben in Ziffer 2 verpflichtet wurde.
Diese Verpflichtung auf das Datengeheimnis besteht auch nach Beendigung des Auftragsverhältnisses oder dem Ausscheiden des Mitarbeiters beim Auftragnehmer fort.

3.1.5 Sofern aufgrund des Gegenstandes der Wartungsarbeiten die Kenntnis und Verarbeitung von personenbezogenen Daten unvermeidbar ist (z.B. durch Zugriff auf DV- Systeme, medizintechnische Geräte mit gespeicherten Patientendaten) ist vor Durchführung der

Wartungsarbeiten ein Auftragsverarbeitungsvertrag gem. Art 28 DSG-VO abzuschließen.

3.1.6 Bei groben Verstößen gegen das Datengeheimnis und/oder die Datensicherheit wird eine Vertragsstrafe von 25.000 Euro festgesetzt. Darüber hinaus sehen das Bundesdatenschutzgesetz und andere einschlägige Rechtsvorschriften Geld- oder Freiheitsstrafen für diesen Fall vor.

3.1.7 Der Auftragnehmer hat bei Verdacht eines Datenschutz-Verstoßes durch einen seiner Mitarbeiter im Rahmen vertraglicher Arbeiten den Auftraggeber unverzüglich zu informieren.

3.1.8 Protokollierung
Jeder Wartungsvorgang muß schriftlich protokolliert werden und ein Duplikat dieser Aufzeichnungen dem Auftraggeber ausgehändigt werden.
Das Protokoll muß enthalten:
- Beschreibung der durchgeführten Arbeiten
- Beginn und Ende der Wartungsarbeit (Tag und Uhrzeit)
- Namentliche Nennung des Wartungspersonals
- Nennung evtl. veränderter Dateien und Programme
- Angabe einer Rufnummer, unter der man den Auftragnehmer bei Schwierigkeiten aufgrund der Änderung jederzeit erreichen kann.

3.1.9 Datensicherheit:
Der Auftragnehmer hat dafür zu sorgen, daß bei der Ausführung der ihm übertragenen Aufgaben die erforderliche Datensicherheit gewährleistet ist. Unter Datensicherheit versteht man alle technischen und organisatorischen Maßnahmen zum Schutz von Daten vor unbefugter Kenntnisnahme, Verfälschung, Zerstörung und unzulässiger Weitergabe.

3.1.9.1 Datensicherung vor der Wartung
Der Auftragnehmer hat das zuständige Personal des Klinikums darauf hinzuweisen, vor Beginn der Wartungsarbeiten eine Datensicherung durchzuführen, wenn dies notwendig ist.

3.1.9.2 Virenprüfung
Vom Auftragnehmer mitgebrachte Datenträger müssen frei von Schadsoftware sein, d.h. sie sind vor ihrem Einsatz beim Auftraggeber mit einem Virenschutzprogramm aktuellen Stands auf Schadsoftwarefreiheit zu prüfen.
Ebenso sind Daten und Programme zu prüfen, bevor sie auf dem Fernleitungsweg zum Auftraggeber übertragen werden.

3.1.9.3 Softwaretest
Softwaretests dürfen nur mit Testdaten durchgeführt werden. Programmänderungen dürfen nur nach gründlichem Test in nichtoperativer Umgebung zum Einsatz kommen.
Werden Softwaretests nicht beim Auftraggeber selbst durchgeführt, sondern auf Anlagen des Auftragnehmers, so dürfen keinesfalls Testdaten aus personenbezogenen Echtdaten, sondern nur anonyme Beispiel-Testdaten verwendet werden.

3.2 **Besondere Anforderungen bei Fernwartung**
Fernwartung sollte nur dann eingesetzt werden, wenn eine Wartung vor Ort aus wirtschaftlichen Gründen nicht vertretbar ist oder aus anderen zwingenden Gründen notwendig ist.
Bei der Fernwartung von informationsverarbeitenden Systemen oder medizinisch-technischen Geräten sind folgende Punkte einzuhalten:

- Sofern aufgrund des Gegenstandes der Fernwartungsarbeiten die Kenntnis und Verarbeitung von personenbezogenen Daten unvermeidbar ist (z.B. durch Zugriff auf DV- Systeme, medizintechnische Geräte mit gespeicherten Patientendaten) ist vor Durchführung der Fernwartung ein Auftragsdatenverarbeitungsvertrag gem- Art. 28 DSGVO abzuschließen.
- Die Fernwartung darf ausschließlich über den offiziellen, gesicherten Fernwartungszugang des Auftraggebers erfolgen. Der Zugang wird über die Abteilung für Informationsverarbeitung oder der Abteilung für Technik des Klinikums Nürnberg eingerichtet.
- Der Auftragnehmer hat Maßnahmen gegen eine mißbräuchliche Benutzung der Fernwartungsverbindung zu treffen.
- Die Fernwartungsverbindung muß vom Auftraggeber jederzeit - in Absprache mit dem Auftragnehmer - unterbrochen werden können.
- Die Wartungsvorgänge müssen vom Personal des Auftraggebers synchron mitverfolgt werden können; wo dies nicht möglich ist, sind **alle** Wartungsaktivitäten elektronisch zu protokollieren und dem Auftraggeber zugänglich zu machen, so daß für Zwecke der Datenschutzkontrolle erkennbar ist, auf welche Datensätze zugegriffen wurde.
- Der Fernwartungszugang zum freigeschalteten Zielrechner darf vom Auftragnehmer nicht dazu benutzt werden, unbefugt andere DV-Systeme des Auftraggebers anzusteuern.
- Die Mitarbeiter sind entsprechend der in Ziffer 2 genannten Vorgaben zur Verschwiegenheit zu verpflichten.

4. Mitwirkungspflichten zur Wahrung und Erfüllung von Betroffenenrechten nach Art. 12- 23 DSGVO
Der Auftragnehmer ist verpflichtet, den Auftraggeber durch geeignete technische und organisatorische Maßnahmen dabei zu unterstützen, Anträge von Betroffenen nach Art 12- 23 DSGVO

- auf Auskunft
- auf Löschen
- auf Information
- auf Sperren
- auf Herausgabe
- auf Ausübung des Widerspruchsrechts

nachzukommen.

5. Leihgeräte
Der Auftragnehmer verpflichtet sich, bei leihweise dem Auftraggeber zur Verfügung gestellten Geräten, die evtl. auf diesen Geräten gespeicherten personenbezogenen Daten unverzüglich nach Rückgabe der Geräte unwiderruflich zu löschen, keine Kopien anzufertigen und dies auf Anfrage dem Auftraggeber schriftlich zu bestätigen und nachzuweisen.