Datenschutzvereinbarung zwischen

_____

_____

_____

_____

(im nachfolgenden „Auftraggeber“ genannt)

und der

GSG Consulting GmbH
-vertreten durch deren Geschäftsführer, Herrn Dr. Andreas Lang-
Flughafenring 2
44319 Dortmund

(im nachfolgenden „GSG“ genannt)

Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Dienstvertrag/ Werkvertrag (Hauptvertrag) in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Dienstvertrag/ Werkvertrag (Hauptvertrag) in Zusammenhang stehen und bei denen Mitarbeiter der GSG oder durch die GSG beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrags.

Thema: Hauptvertrag:

Datum:

Sofern kein Hauptvertrag besteht, bezieht sich die Datenschutzvereinbarung auf folgendes Projekt:

VIPP-Projekt_____
_____

(im nachfolgenden „Projekt“ genannt).

§ 1 Definitionen

(1) Personenbezogene Daten
Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

(2) Datenverarbeitung im Auftrag
Datenverarbeitung im Auftrag ist die Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung personenbezogener Daten durch die GSG im Auftrag des Auftraggebers.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Die GSG verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag oder im Projekt konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an die GSG sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („verantwortliche Stelle“ im Sinne des § 3 Abs. 7 BDSG).

(2) Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages oder Projektes und nach Beendigung die Berichtigung, Löschung, Sperrung und Herausgabe von Daten verlangen.
(3) Die Inhalte dieser Vertragsanlage gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird, und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 3 Pflichten der GSG

(1) Die GSG darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

(2) Die GSG wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Forderungen des Bundesdatenschutzgesetzes (§ 9 BDSG) entsprechen. Dies beinhaltet insbesondere:

a) Unbefugten den Zutritt zu Datenverarbeitungsanlagen,mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),

b) zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

c) dafür Sorge zu tragen, 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 (Zugriffskontrolle),

d) dafür Sorge zu tragen, 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 (Weitergabekontrolle),

e) dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. (Auftragskontrolle),

f) dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

g) dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).
Eine Maßnahme nach b bis d ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.
Eine Darstellung dieser technischen und organisatorischen Maßnahmen wird Anhang zu dieser Anlage.

(4) Die GSG stellt auf Anforderung dem Auftraggeber die für die Übersicht nach § 4g Abs. 2 S. 1 BDSG notwendigen Angaben zur Verfügung.

(5) Die GSG stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß § 5 Bundesdatenschutzgesetz (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes eingewiesen worden sind. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

(6) Der Datenschutzbeauftragte der GSG ist Herr Rechtsanwalt Stefan Strüwe in Münster.

(7) Die GSG unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers.

(8) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Die GSG hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Die GSG ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt die GSG auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

(9) Die Erfüllung der vorgenannten Pflichten ist von GSG zu kontrollieren und in geeigneter Weise nachzuweisen.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber und die GSG sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

(2) Der Auftraggeber hat die GSG unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Die Pflicht zur Führung des öffentlichen Verfahrensverzeichnisses (Jedermannverzeichnis) gem. § 4g Abs. 2 S. 2 BDSG liegt beim Auftraggeber.

(4) Dem Auftraggeber obliegen die aus den für ihn geltenden Datenschutzbestimmungen resultierenden Informationspflichten.

(5) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

(6) Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, die über das nomale Maß hinaus gehen , so trägt diese der Auftraggeber.

(7) Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

§ 5 Anfragen Betroffener an den Auftraggeber

Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der GSG den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen, vorausgesetzt:
-der Auftraggeber hat die GSG hierzu schriftlich aufgefordert und
-der Auftraggeber erstattet die GSG die durch diese Unterstützung entstandenen Kosten.

§ 6 Kontrollpflichten

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen der GSG und dokumentiert das Ergebnis. Hierfür kann er Selbstauskünfte bei der GSG einholen und sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich überzeugen.
(2) Die GSG verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers bei der GSG durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat die GSG den Auftraggeber unverzüglich darüber zu informieren. Die GSG wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortlicher Stelle“ im Sinne des Bundesdatenschutzgesetzes liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen der GSG - bedürfen einer schriftlichen Vereinbarung 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.

(3) Es gilt deutsches Recht.

Dortmund, den _____

_____ _____
GSG Consulting GmbH Einrichtung

Anhang 1
Auflistung der personbezogenen Daten und Zweck ihrer Verarbeitung durch die GSG im Auftrag des Auftraggebers.

- ☒ Daten §21 KHEntgG.
- ☐ Patientendaten (Papier oder Digital)
- ☐ Sonstige:_____

Anhang 2
Darstellung der technischen und organisatorischen Maßnahmen der GSG.

1. Zutrittskontrolle zu den Räumlichkeiten der GSG:

GSG-Server beim Rechenzentrum:

- Legitimationsprüfung aller Rechenzentrumsbesucher und Dokumentation aller Besuche durch autorisierte GSG-Mitarbeiter.
- Sicherheits-Rundschleuse mit Zutrittsvereinzelung und elektronischen Gewichtssensoren.
- Tokenbasierte Schließanlage.
- Sensorgesteurte Überwachung aller Türen und rechenzentrumsrelevanter Räume.
- Permanente Videoüberwachung mit Aufzeichnung und Speicherung.
- Bewegungsmelder und Einbruchmelder mit direkter Aufschaltung zu einem Sicherheitsdienst.

GSG-Räume (Dortmund):

- Verschlossene Tür
- Objektschutz durch Sicherheitsdienst und direkt Lage an Polizeidienststelle
- Permanente Videoüberwachung im gesamten Flughafengebäude
- Verschlossene Schranktüren

2. Zugangskontrolle

- Nutzung sicherer Kennwörter und Zertifikate
  (Festlegung in interner Organisationsvereinbarung).
- Firewall (kann bei Bedarf näher spezifiziert werden).
- Zugriff zum Rechenzentrum aussschließlich über VPN
- Festplatten Verschüsselung mit pre boot Authentifizierung

3. Zugriffskontrolle

- Zugriff nur durch autorisierte GSG-Mitarbeiter

- Detailregelungen in den internen Organisationsvereinbarungen zum Eintritt und Austritt
- Die GSG verfügt seit über 10 Jahren über ein DIN EN ISO zertfiziertes Managementsystem

4. Weitergabekontrolle

Übertragungskontrolle:

- Festplatten Verschüsselung
- Upload-Portal SSL verschlüsselt
- bei Versand per E-Mail Verschlüsselung der Anhänge (z.B. PGP)
- Firewall
- Virenschutz

Transportkontrolle:

- Bei Verwendung von Datenträgern nur mit geschützen Dateien
- Patienten-Akten in verschlossenen Behältnissen

5. Eingabekontrolle

Protokollierung von:

- Log-In / Log-Out
- Änderung von Passwörtern
- Änderung der Zugriffsrechte
- Schreibende Zugriffe auf Dateien und Datenbanken

6. Auftragskontrolle

- Vereinbarung gemäß §11 BDSG mit externen Unternehmen

7. Verfügbarkeitskontrolle

- Sicherung des Serverraums nach Vorgaben des BSI
- Redundantes Speichersystem mit Fehler- Erkennung und Fehler-Toleranz
- Lagerung der Sicherungsdateien in getrennten Brandabschnitten
- Backups auf externe Sicherungsmedien

8. Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Uploadportal mit zweckgebundenden unterschiedlichen Uploadbereichen
- Speicherung und Weiterverarbeitung in getrennten Speicherorten.