Anlage 1: Leistungsbeschreibung

Die Tätigkeiten des Auftragnehmers für den Auftraggeber im Rahmen der Auftragsverarbeitung sind wie folgt festgelegt (Mehrfachnennungen sind möglich):

In Auftrag gegeben wird die Herstellung von Jubiläumsurkunden. Hierfür werden die erforderlichen Daten erhoben, zwischengespeichert sowie bis zum finalen Druck verarbeitet.

Nach der Erstellung der Urkunde verbleiben die Daten noch für 3 Jahre beim Auftragnehmer, sollte eine erneute Ausstellung derselben Urkunde notwendig sein. Danach werden die Daten automatisch gelöscht.

Anlage 2: Betroffene und Datenkategorien

Der Auftragnehmer verarbeitet vertragsgemäß auch personenbezogene Daten für den Auftraggeber. Diese werden im Folgenden spezifiziert. Bedingt durch den technologischen Wandel und organisatorische Veränderungen kann sich die Zusammensetzung der Daten auch verändern.

☒ **Beschäftigte** ☒ **ehemalige Beschäftigte**

- Name und Vorname des Jubilars,
- Eintrittsdatum,
- Unternehmensname
- Kontaktdaten des Ansprechpartners im Unternehmen

Anlage 3: Technische und organisatorische Schutzmaßnahmen

Bei der Verarbeitung personenbezogener Daten sind technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Datenschutzes zu gewährleisten:

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- *die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*
- *die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*
- *die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*
- *ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.*

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

[Artikel 32 DS-GVO]

Es sind insbesondere – aber nicht abschließend – die nachfolgenden Vorgaben zu beachten:

Diese technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es der datenempfangenden Gesellschaft gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber anzuzeigen.

Sofern eine direkte Personenbeziehbarkeit nicht erforderlich ist, ist von den Möglichkeiten der Pseudonymisierung Gebrauch zu machen, wenn dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (Datensparsamkeit).

Nicht länger benötigte Daten müssen rechtzeitig sicher gelöscht werden, z. B. wenn eine gesetzliche Regelung besteht, die eine Löschung vorsieht und/oder keine Aufbewahrungspflicht besteht.

Die Übertragung von personenbezogenen Daten ist zu schützen. Die Klassifikationsstufe der jeweiligen Informationen ist bei der Form des Datenaustauschs entsprechend zu berücksichtigen. Sollten im Rahmen des gleichen Datenaustauschs Informationen mit unterschiedlichen Klassifikationsstufen an einen Kommunikationspartner übermittelt werden, dann ist für den gesamten Datenaustausch das Schutzniveau der höchsten Klassifikationsstufe zu nutzen. Die Übertragung sensibler/vertraulicher Daten ist ausschließlich in verschlüsselter Form zulässig.

Die Zugangsberechtigungen sind auf die für die Aufgabenerfüllung notwendigen Rechte zu beschränken (Minimalprinzip). Nach Erfüllung der Aufgabe sind die Berechtigungen zu löschen oder zu sperren. Die Rechtebeantragung unterliegt der Pflichtentrennung. Die Vergabe ist zu dokumentieren.

Sofern ein Zugriff auf das System des Auftraggebers stattfindet, sind diese Zugangsrechte für Mitarbeiter des Auftragnehmers beim Auftraggeber per E-Mail unter Nennung der Gründe und des Umfangs der

Rechte zu beantragen bzw. der Auftraggeber ist rechtzeitig vorher zu informieren. Sollte der Zugriff auf personenbezogene Daten nicht zwingend erforderlich sein, so ist hierauf zu verzichten. Die Rechte sind in Lese- und Schreibrechte zu unterscheiden. Der Zugriff über externe Netze ist entsprechend zu schützen (Verschlüsselung, Authentifizierung etc.: siehe unten).

Es sind sichere Kennwortverfahren nach dem aktuellen Stand der Technik (beispielsweise gemäß Empfehlungen des BSI) eingerichtet. Datenverarbeitungssysteme werden gesperrt, wenn diese unbeaufsichtigt sind. Es sind Maßnahmen der Zwei-Faktor-Authentifizierung zu prüfen.

Wenn Daten/Unterlagen nicht unter Aufsicht/Kontrolle der zuständigen Mitarbeiter sind, sind sie unter Verschluss aufzubewahren und beim Transport entsprechend des Schutzbedarfs sicher zu transportieren; hierzu sollten mobile Datenträger verschlüsselt werden.

Die Daten sind entsprechend zu ihren Zwecken getrennt zu verarbeiten. So sind die vorgegebenen Systeme zu nutzen und keine Datenexporte vorzunehmen, um Daten unterschiedlicher Systeme/Zweckbestimmungen zusammenzuführen (z. B. in Excel).

Auch ist Unbefugten der Zutritt zu den Räumlichkeiten zu verwehren. Hierunter fallen neben dem Serverraum auch die weiteren Räume, in denen sich Datenverarbeitungsanlagen befinden, die einen Zugang zu den Systemen ermöglichen. Zutritt ist nur für bestimmte, berechtigte Zwecke erlaubt. Hierbei sind auch Personen von Dienstleistern entsprechend zu berücksichtigen. Zur Zutrittskontrolle gehören ferner u. a. folgende Maßnahmen:

- Zutrittskontrollsystem
- Türsicherung (elektrische Türöffner usw.)
- Werkschutz, Pförtner
- Überwachungseinrichtung
- Alarmanlage

Datenträger, die schützenswerte Daten enthalten und nicht mehr gebraucht werden oder aufgrund eines Defektes ausgesondert werden sollen, sind so zu entsorgen, dass keine Rückschlüsse auf vorher gespeicherte Daten möglich sind; bis zur Vernichtung sind diese sicher zu verwahren, dass Unbefugte auf die Unterlagen nicht zugreifen können. Analoges gilt für Belege und Druckausgaben.

Die Zugangsprotokolle umfassen erfolgreiche/erfolglose Logins und vom Benutzer bzw. dem System initiierte Logins. Systemsicherheitsrelevante Aktivitäten (alle Aktivitäten im Administrator-Modus) sind stets zu protokollieren. Die Protokolldaten sind manipulationssicher, zeitnah verfügbar und gemäß den gesetzlichen Anforderungen aufzubewahren. Der Zugriff auf Protokolldaten ist nur autorisierten Benutzern zu gestatten. Die Protokolldaten sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Um Sicherheitslücken in den IT-Systeme zu schließen, sind zeitnah Sicherheits-Updates und -Patches einzuspielen. Hierbei sind mobile Geräte bzw. nicht dauerhaft mit dem internen IT-Netzwerk verbundene Geräte ebenfalls zu berücksichtigen.

Dateneingaben, -veränderungen und -löschungen sind zu protokollieren. Diese sind regelmäßig auf unbefugte Datenverarbeitungsvorgänge zu prüfen.

Es sind angemessene Maßnahmen zu ergreifen, die die Unversehrtheit der Daten und der Programme vor Fälschung, Vernichtung und Änderung sicherstellen. Auch sind Maßnahmen einzuführen, die fehlerhafte Daten als solche erkennen. So sind u. a. eingehende Daten (z. B. E-Mails oder Datenträger) auf Viren zu prüfen und die Mitarbeiter entsprechend zu sensibilisieren). Die Firewall ist so zu konfigurieren und zu administrieren, dass sie einen effektiven Schutz darstellt und Manipulationen verhindert werden.

Um das Risiko eines Datenverlusts zu reduzieren, sind regelmäßige Datensicherungen durchzuführen. Ferner sind die Datenverarbeitungssysteme entsprechend zu warten und zu aktualisieren. Ferner gehören zur Verfügbarkeitskontrolle u. a. folgende Maßnahmen:

- » Backup-Verfahren
- » Spiegeln von Festplatten
- » Unterbrechungsfreie Stromversorgung (USV)
- » Getrennte (räumliche) Aufbewahrung der Datensicherungen
- » Virenschutz / Firewall

Alle sicherheitsrelevanten Vorfälle (z. B. unerklärliches Systemverhalten, Verlust oder Änderung von Daten und Programmen, Verfügbarkeit nicht explizit freigegebener Dienste, Verdacht des Missbrauchs der eigenen Benutzerkennung etc.) müssen dem Auftraggeber sofort gemeldet werden. Es sind Maßnahmen für Notfall-, Katastrophen- und Wiederanlaufplanung zu erstellen.

Es hat eine regelmäßige Überprüfung hinsichtlich der Wirksamkeit der für Notfall-, Katastrophen- und Wiederanlaufplanung getroffenen Maßnahmen stattzufinden. So sollte in regelmäßigen Abständen eine Analyse durchgeführt werden, die die derzeitigen Schwächen und Schwachstellen aufdeckt. Darauf aufbauend sind Maßnahmen zur Beseitigung zu erarbeiten. Darüber hinaus ist eine Risikoanalyse durchzuführen, um die Risiken hinsichtlich des Geschäfts aufzudecken und bei den IT-Sicherheitsmaßnahmen zu berücksichtigen.

Es ist sicherzustellen, dass die Einhaltung der Datenschutzgrundsätze nachgewiesen werden kann (Rechenschaftspflicht). Es sind geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß den datenschutzrechtlichen Vorschriften erfolgt. Dies bedeutet, dass beweissicher dokumentiert werden muss, was zur Einhaltung der datenschutzrechtlichen Vorgaben unternommen wird.

Es ist in regelmäßigen Abständen ein Audit oder eine Revision der festgelegten technischen und organisatorischen Maßnahmen durchzuführen, die die derzeitigen Schwächen und Schwachstellen aufdeckt. Darauf aufbauend sind Maßnahmen zur Beseitigung zu erarbeiten. Darüber hinaus sollte eine Risikoanalyse durchgeführt werden, um die Risiken hinsichtlich des Geschäfts aufzudecken und bei den IT-Sicherheitsmaßnahmen zu berücksichtigen.

Anlage 4: Betriebliche Datenschutzbeauftragte

Datenschutzbeauftragter des Auftraggebers:

Name:	UIMC Dr. Voßbein GmbH & Co KG
Anschrift:	Otto-Hausmann-Ring 113, 42115 Wuppertal
Telefonnummer:	+49 202 946 7726 200