Vereinbarung

zwischen

_____

Unternehmen

_____

vertreten durch

_____

Straße / Hausnummer

_____

PLZ/ Ort

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

IllusionFACTORY, Herr Martin Schneider, Max-Planck-Straße 15,53819 Neunkirchen-Seelscheid

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand
Der Gegenstand des Auftrags ergibt sich aus dem Angebot 1712006 vom 18.12.2017, auf das hier verwiesen wird (im Folgenden Leistungsvereinbarung). Insoweit ist die Bereitstellung von Webhosting-Dienstleistungen sowie der damit im Zusammenhang stehenden Leistungen wie z.B. E-Mail, Domainregistrierung Gegenstand des Vertrages. Für das Web- und Mail-Hosting wird dem Auftraggeber Speicherplatz auf Servern innerhalb der Bundesrepublik Deutschland zur Verfügung gestellt. Eine evtl. Verlagerung der Datenverarbeitung in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers. Die Daten werden in einer Datenbank verwaltet.
Im Rahmen dieses Vertrages hat der Auftraggeber die Möglichkeit, Daten zu verarbeiten (zu speichern, zu verändern, zu übermitteln und zu löschen).
Die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer ist **nicht** Gegenstand des Vertrages. Jedoch kann ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden bei der der Leistungserbringung des Auftragnehmers im Rahmen des Hostings, des Supports bzw. der Administration von Server-Systemen für den Auftraggeber.

(2) Dauer
Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 1 Monat nach 36 Monaten gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Die Daten werden verarbeitet um für den Auftraggeber die Website ordnungsgemäß zu hosten und die Mail-Kommunikation zu ermöglichen. Die Verarbeitung umfasst 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 von Daten.
Ein Zugriff auf personenbezogener Daten und anderer schutzwürdiger Daten kann im Rahmen der Dienstleistung nicht ausgeschlossen werden.

(2) Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):
- Kommunikationsdaten (Name, Telefon-Nr., E-Mail-Adressen)
- Nutzungsdaten (Protokollierung der Nutzeraktivitäten, Log-Files, IP-Adressen)
- Inhaltsdaten (Internet-Kontaktformular, E-Mail-Nachrichten)

(3) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
- Webseitenbesucher
- Interessenten und Kunden
- Abonnenten

- Beschäftigte
- Lieferanten
- Newsletter- Abonnenten

des Auftraggebers.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].
(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☐ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

- ☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- ☐ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
- ☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) ☒ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr Martin Scheider [martin.schneider@illusion-factory.de, Telefon: 02247 30201-0] benannt.

c) ☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

d) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

h) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

i) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☒ Der Auftraggeber stimmt der Beauftragung der von Unterauftragnehmern zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO nach billigem Ermessen der Auftragnehmers zu.

c) ☒ Die Auslagerung auf Unterauftragnehmer oder

☒ der Wechsel des bestehenden Unterauftragnehmers

sind nach billigem Ermessen unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zulässig.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

☒ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

☒ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
☐ Durch Vorlage eines Berichts oder einer Bestätigung des Datenschutzbeauftragten.

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Haftung

Bezüglich der Haftung wird auf Art. 82 DS-GVO verwiesen.

12. Sonstiges

(1) Änderungen dieser Auftragsverarbeitungsvereinbarung bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung dieser Bedingungen handelt.
(2) Es gilt die Datenschutzgrundverordnung (DS-GVO), Bundesdatenschutzgesetz sowie deutsches Recht.
(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Auftraggeber:

Ort, Datum	Name in Druckbuchstaben	Unterschrift

Auftragnehmer:

Ort, Datum	Name in Druckbuchstaben	Unterschrift

Anlage 1 – Technisch-organisatorische Maßnahmen

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO
(Stand: 13.10.2018)
der

IllusionFACTORY
Inhaber: Dipl.-Inf. Martin Schneider
Max-Planck-Straße 15
53819 Neunkirchen-Seelscheid

Unternehmen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben technischen und organisatorischen Maßnahmen umzusetzen, damit die Verarbeitung im Einklang mit den datenschutzrechtlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird. Das o.g. Unternehmen hat folgende konkrete TOMs zur Gewährleistung von Datenschutz und Datensicherheit getroffen:

Inhalt:

1 Vertraulichkeit (Geheimhaltung)

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

Technische Maßnahmen		Organisatorische Maßnahmen	
✓	Gebäude außerhalb Bürozeiten abgeschlossen	✓	Schlüsselregelung / Liste für Haus-, Etagen- und Servertüren
	Alarmanlage für Haustüre und Hauptflur		Richtlinie zur Begleitung von Besuchern
✓	Manuelles Schließsystem		Besucherbuch mit Protokollierung
✓	Sicherheitsschlösser		Empfang vorhanden
	Klingelanlage	✓	Reinigungsdienst sorgfältig ausgewählt
	Eigene Serverräume verschlossen		
	Gesicherte Fenster		

1.1.1 Zugangskontrolle

Maßnahmen, die verhindern das Datenverarbeitungs-Systeme (Hardware, Betriebssystem, Software-Anwendung) von Unbefugten genutzt werden können.

Technische Maßnahmen		Organisatorische Maßnahmen	
✓	Login mit Benutzername + Passwort		Allgemeine Datenschutz-/Datensicherheit Richtlinie
✓	Techn. Passwort-Prüfung 4 aus 4	✓	Passwort-Richtlinie vorhanden
✓	Anti-Viren-Software Server		Vorgabe manuelle Desktopsperre
✓	Anti-Viren-Software Clients	✓	Bei Verlassen des Arbeitsplatzes wird Bildschirm gesperrt
✓	Firewall		
	(Intrusion Detection-System) aktiviert		
✓	VPN bei Remote-Zugriffen		
✓	Eindeutige Zuordnung der Benutzerkonten. Keine unpersönlichen Sammelkonten.		
	Benutzerkontosperre nach 3 fehlgeschlagenen Anmeldeversuchen		
✓	Automatische Desktopsperre		
✓	Techn. Dokumentation der Zugangsberechtigungen		
	Sperrung externer Schnittstellen (USB)		

1.1.2 Zugriffskontrolle

Maßnahmen, die verhindern, dass unerlaubte Tätigkeiten innerhalb von IT-Systemen durchgeführt werden. Es handelt sich z.B. um Lesen, Kopieren, Verändern, und Entfernen von Daten außerhalb eingeräumter Berechtigungen.

Technische Maßnahmen		Organisatorische Maßnahmen	
	Trennung von Berechtigungs-bewilligung und Berechtigungs-vergabe		Berechtigungskonzept (need-to-know-Prinzip)
✓	Aktenshredder	✓	Minimale Anzahl Administratoren
	Externe Aktenvernichtung	✓	Konzept zur Laufwerksnutzung
✓	Datenträgerlöschung		
✓	Netzlaufwerk mit Zugriffs-möglichkeiten nur für Berechtigte		
	Protokollierung von Zugriffen		

1.1.3 Trennungskontrolle

Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobenen Daten auch getrennt verarbeitet werden.

Technische Maßnahmen		Organisatorische Maßnahmen	
✓	Berechtigungskonzept ermöglicht getrennte DV der Mandanten/Kunden (separates Laufwerk)	✓	Trennung durch unterschiedliche Mitarbeiter
	Physische Trennung Datenträger		
✓	Trennung von Produktiv- und Testumgebung		

1.1.4 Pseudonymisierung

Maßnahmen, damit Personen nur mit zusätzlichen Informationen identifiziert werden können. Unterstützt den Grundsatz der Datenminimierung und privacy bei default.

Technische Maßnahmen		Organisatorische Maßnahmen	
	Löschung bestimmter Daten		Interne Anweisung vor Datenweitergabe Daten zu pseudonymisieren auf Wunsch möglich
✓	Benutzername für Mailkonto ist pseudonymisiert		

1.1.5 Verschlüsselung

Maßnahmen zum Schutz von Daten gegen unbefugte Kenntnisnahme oder absichtliche Manipulation

Technische Maßnahmen		Organisatorische Maßnahmen	
✓	Eine Verschlüsselung von Notebooks		Arbeitsanweisung zur manuellen Verschlüsselung
	USB-Stick-Verschlüsselung		
	ROM-Laufwerke gesperrt		
	Verschlüsselung von Mail-Anhängen		
	Verschlüsselung von Mail-Inhalten		
✓	Verschlüsselter Internet-Auftritt		
✓	Gesichertes WLAN		

2 Integrität (Korrektheit und Unverfälschbarkeit)

2.1.1 Eingabekontrolle

Maßnahmen, um die Dateneingabe, -Veränderung und Entfernung nachzuweisen.

Technische Maßnahmen		Organisatorische Maßnahmen	
	Technische Protokollierung in den Anwendungen	✓	Aufbewahrung von Papierformularen, von den Daten in IT-Systemen übernommen werden
	Technische Protokollierung der Administratorentätigkeit	✓	Klare Zuständigkeiten für Datenlöschung
	Archivierung von Anforderungen zur Berechtigungsvergabe		Vertragliche Beschränkung des tätigen Mitarbeiterkreises
	Archivierung von Anforderungen zur Passwortrücksetzung		

2.1.2 Weitergabekontrolle

Maßnahmen, um die elektronischen Übertragungen und den Datentransport zu sichern.

Technische Maßnahmen		Organisatorische Maßnahmen	
	Verschlüsselter Datenträgertransport		Sorgfältige Auswahl von Transportpersonal
	Datenaustausch über die zur Verfügung gestellte Internet- Plattform PKM		Gesicherte Transportbehälter
✓	Client-Zugriff auf e-Mails über HTTPS bzw. SSL-Verschlüsselung		Arbeitsanweisung zum Verschlüsseln
✓	Verschlüsselte VPN-Verbindung		Persönliche Übergabe mit Protokoll
✓	Mail-Transportverschlüsselung		
	Mail-Anhangverschlüsselung		

3 Verfügbarkeit, Belastbarkeit und schnelle Wiederherstellbarkeit

Maßnahmen, um die Daten gegen Verlust und Zerstörung zu schützen.

Technische Maßnahmen		Organisatorische Maßnahmen	
✓	Datensicherungen	✓	Backup- /Recoverykonzept
✓	Feuer- und Rauchmelder	✓	Daten-Wiederherstellung wird regelmäßig getestet
	CO2-Feuerlöscher Serverraum		
	Serverraum klimatisiert		
	Volumen Schattenkopie automatisiert ca. alle 6 Stunden	✓	Aufbewahrung der Datensicherungen im abschließbaren Schrank außerhalb des Serverraums

✓	USV	✓	Keine sanitären Anschlüsse im Serverraum
✓	Einsatz von Schutzprogrammen (Virenscanner, Firewall, Spamfilter u.a.)	✓	Manuelle und automatisierte Überwachung von Schutzprogrammen
✓	Festplattenspiegelung		

4 Weitere Maßnahmenbereiche

4.1.1 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Technische Maßnahmen		Organisatorische Maßnahmen	
✓	Es werden nicht mehr Daten erhoben als für den Zweck erforderlich ist.		
✓	Daten werden nur so lange gespeichert wie für Zweck erforderlich		
✓	Keine Zugriffsmöglichkeit durch Dritte		

4.1.2 Auftragskontrolle

Maßnahmen, die sicherstellen, dass Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Technische Maßnahmen		Organisatorische Maßnahmen	
	Externe verarbeiten die Daten ausschließlich in Räumen der IllusionFACTORY		Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
		✓	Sorgfältige Auswahl von Auftragnehmern
		✓	Eindeutige Vertragsgestaltung gem. Art. 28 DSGVO
			Verpflichtung der Mitarbeiter auf Datengeheimnis
			Keine Auftragsverarbeitung ohne Weisung

4.1.3 Datenschutz-Managementsystem

Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Technische Maßnahmen		Organisatorische Maßnahmen	
	Zentrale Dokumentation der Verarbeitungstätigkeiten	✓	Externer Datenschutzbeauftragter nicht erforderlich
	Durchführung von Penetrationstests	✓	Datenschutzverantwortung ist festgelegt
		✓	Mitarbeiter auf Datengeheimnis verpflichtet

			Mitarbeiter werde regelmäßig geschult/sensibilisiert
			Jährliche Überprüfung der TOMs

4.1.4 Incident-Response-Management

Maßnahmen, die Sicherheitsvorfälle/IT-Angriffe erkennen und beseitigen.

Technische Maßnahmen		Organisatorische Maßnahmen	
✓	Einsatz von Firewall mit regelmäßiger Aktualisierung		Dokumentierte Vorgehensweise für evtl. Sicherheitsvorfälle
✓	Spamfilter mit regelmäßiger Aktualisierung	✓	Einbindung des DSB und IT-Spezialisten
✓	Virenscanner mit regelmäßiger Aktualisierung	✓	Dokumentation von Sicherheitsvorfällen und Datenpannen
		✓	Schulung des Admin-Personals

_____ _____

Datum / Auftraggeber Datum / Auftragnehmer