Anlage: Technische und organisatorische Maßnahmen (IT- und Datenschutz-Sicherheitskonzept) der d.velop AG

d.velop AG
Schildarpstraße 6–8
48712 Gescher, Deutschland
Fon +49 2542 9307-0
Fax +49 2542 9307-20
d-velop.de
info@d-velop.de

Handelsregister Coesfeld
HRB 4903
USt-IdNr. DE813062165

Vorstand: Christoph Pliete (Vorsitzender),
Mario Dönnebrink
Aufsichtsratsvorsitzender: Dr. Helmut Bäumer

WGZ Bank Münster
DE43 40060000 0002160370
GENO DE MSXXX

Volksbank Gescher eG
DE17 40164901 0057380200
GENO DE M1GE1

VR-Bank Westmünsterland eG
DE77 42861387 0037645400
GENO DE M1BOB

Sparkasse Westmünsterland
DE03 40154530 0053053278
WELA DE 3WXXX

Inhalt

1 Änderungshistorie

Version	Datum	Bearbeiter	Firma/ Abteilung	Bemerkung
1.0.0	29.03.2018	SOCH/SKRE	d.ag; #LOGIN	Neuerstellung gemäß DSGVO
1.0.1	14.03.2018	SOCH	d.ag	Anpassung Gliederung
1.0.2	22.08.2018	SOCH	d.ag	Anpassung Punkt „Verschlüsselung von Funk-Netzwerken“
1.0.3	06.06.2019	SOCH	d.ag	Revision, Anpassung Titel auf „Anlage: Technische und organisatorische Maßnahmen (IT- und Datenschutz-Sicherheitskonzept)“
1.0.4	25.10.2019	SOCH	d.ag	Revision, Anpassung Formatierung und Punkt 2.2.2 Kennwortrichtlinie
1.1.0	30.04.2020	SOCH	d.ag	Revision, Neuformatiertung, Unterteilung in besondere Schutzmaßnahmen für OnPremise und d.velop Cloud, Aktualisierung Punkte unterhalb von 2.1.1, Erweiterung Titel um Firmennamen
1.1.1	06.05.2020	SOCH	d.ag	Überführung Mandantentrennung in eigenen Punkt 4.1.3.1
1.1.2	20.07.2020	SOCH	d.ag	Ergänzung Punkt 2.1.6 Homeoffice und mobiles Arbeiten und Punkt 2.3.7/ 4.3.6 Schwachstellen- und Belastbarkeitstests
1.1.3	02.09.2020	SOCH	d.ag	Anpassung betroffener Produktbereich in Punkt 4.3.3, Ergänzung Punkt 4.3.5 Changemanagement Prozess

2 Allgemeine Schutzmaßnahmen

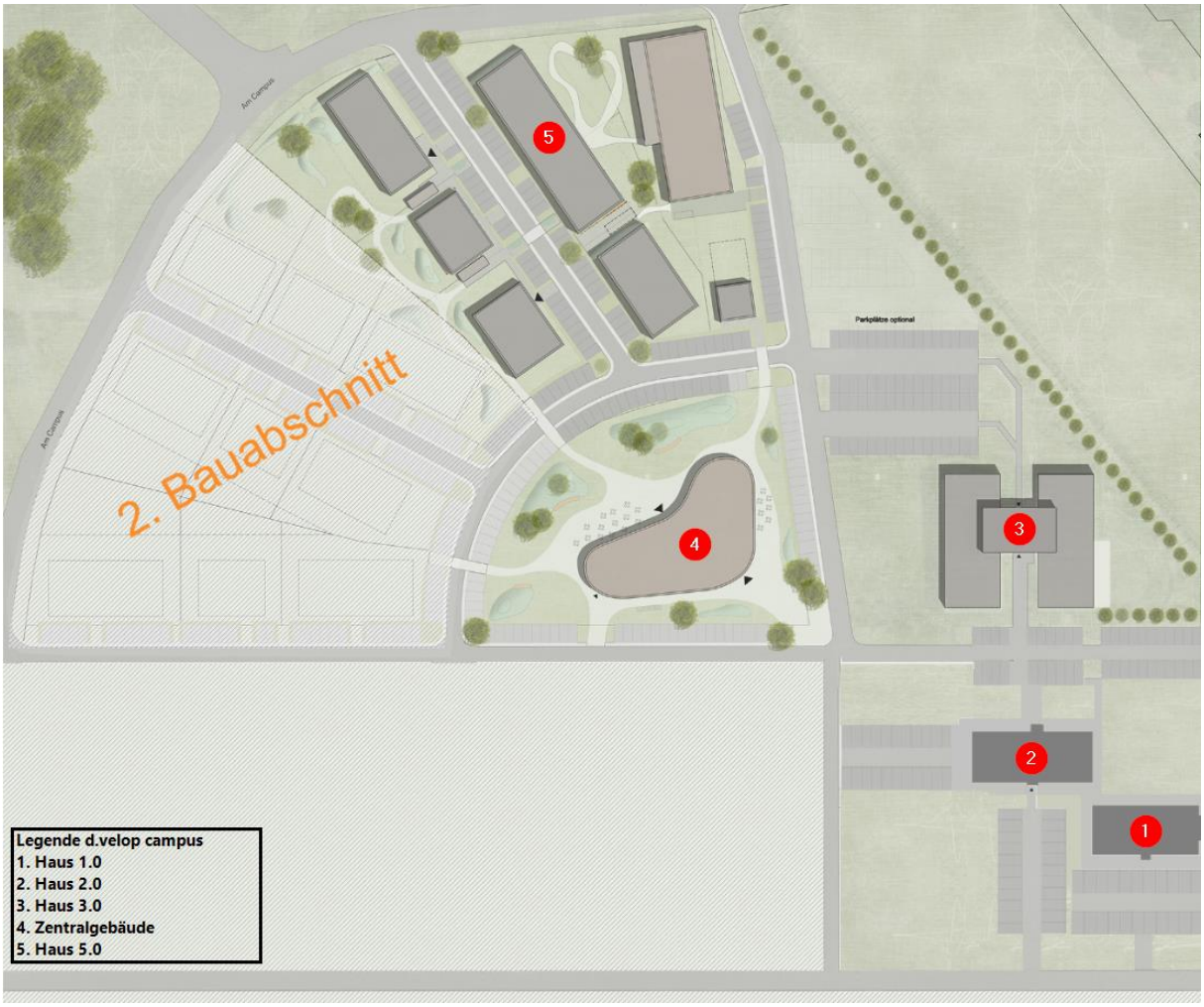
2.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

2.1.1 Zutrittskontrolle

2.1.1.1 d.velop campus

Der d.velop campus befindet sich in der Stadt Gescher, NRW, Deutschland. Der d.velop campus ist nicht eingezäunt und wird nicht videoüberwacht. Alle Gebäude der d.velop AG verfügen über ein Zutrittskontrollsystem und sind mit Bewegungsmeldern und Alarmanlagen ausgestattet. Die Alarmmeldung erfolgt an einen externen Wachdienst.

Die Fassade der Gebäude besteht zum größten Teil aus Glas, so dass die Räume von außen einsehbar sind. Der Support- und Fernwartungsraum befindet sich im 1. Obergeschoss und verfügt über einen zusätzlichen Sichtschutz im Gebäude.



2.1.1.2 Zutrittskontrollsystem

Die d.velop AG verfügt über ein elektronisches Zutrittskontrollsystem. Jeder Mitarbeiter besitzt einen personalisierten Mitarbeiterausweis mit aufgedrucktem Vornamen, Nachnamen, Lichtbild und Firmennamen. Der Ausweis verfügt über bedarfsgerecht vergebene Zutrittsrechte und ermöglicht jederzeit die Sichtkontrolle der Zutrittsberechtigung über das auf dem Ausweis angebrachte Foto. Die d.velop AG verwendet für die Serverräume

spezielle Sicherheitsschlösser, welchen über einen separaten Schließkreis mit separaten Berechtigungen für ausgewählte Mitarbeiter und die Unternehmensleitung verfügen.

2.1.1.3 Verschlossene Gebäude

Der d.velop campus (Firmengelände) besteht insgesamt aus vier Firmengebäuden. Von diesen vier Gebäuden sind drei Gebäude ständig verschlossen. Ein Zutritt ist nur mit einem personalisierten Mitarbeiterausweis möglich (siehe Zutrittskontrollsystem).

Das vierte Gebäude, das Zentralgebäude, ist während der Geschäftszeiten der d.velop AG (07:45 Uhr bis 17:30 Uhr) geöffnet. In diesem Gebäude sind die „öffentlichen" Räume untergebracht, in denen die Besucher (Kunden, Partner, Interessenten, Bewerber, Lieferanten) zu Besprechungen empfangen werden. In diesem Gebäude hat ebenfalls der Empfang seinen Arbeitsplatz, so dass ein Betreten und Verlassen des Gebäudes kontrolliert wird. Das Zentralgebäude wird automatisch um 17:30 Uhr verschlossen.

Zusätzliche Büroflächen sind in einem weiteren Gebäude (Haus 5.0) eingerichtet. Das Gebäude ist ebenfalls ständig verschlossen und ein Zutritt ist auch hier nur mit einem personalisierten Mitarbeiterausweis möglich (siehe Zutrittskontrollsystem).

2.1.1.4 Empfang (Haupteingang)

In Zentralgebäude werden Besucher der d.velop AG empfangen. Der Empfang der d.velop AG ist während der Geschäftszeiten von 07:45 Uhr bis 17:30 Uhr ständig besetzt. Das Empfangspersonal registriert Besucher, händigt den Besuchern einen **Besucherausweis** aus und begleitet die Besucher in die Besprechungsräume. Ein selbständiges Bewegen von Besuchern in den anderen drei Gebäuden ist ausgeschlossen.

2.1.1.5 Workflow zur Erteilung von Zutrittsberechtigungen

Die Zutrittsberechtigungen werden über ein workflowbasiertes System vergeben. Ein Mitarbeiter muss dazu einen elektronischen Zutrittsberechtigungsantrag stellen. In diesem Antrag kann der Mitarbeiter für jedes Gebäude und für jede Sicherheitszone sowohl den Zutritt als auch die Alarmschaltung beantragen. Ein Antrag auf Alarmschaltung umfasst die Scharf-/Unscharfschaltung der Alarmanlage für die angeforderten Gebäude/Sicherheitsbereiche. Der Zutrittsberechtigungsantrag wird **immer** an den direkten Vorgesetzten geleitet. Der Vorgesetzte entscheidet über die Annahme und die Ablehnung des Zutrittsberechtigungsantrags. Sonderberechtigungen werden ausschließlich nach vorheriger Zustimmung der Unternehmensleitung eingeräumt.

2.1.1.6 Bewegungsmelder

Die Gebäude der d.velop AG sind mit Bewegungsmeldern ausgestattet. Die Bewegungsmelder sind mit der Alarmanlage gekoppelt.

2.1.1.7 Gebäudealarmanlage

Die Firmengebäude der d.velop AG sind mit einer Alarmanlage ausgestattet. Neben **einem akustischen Alarmsignal** auf dem Firmengelände der d.velop AG erfolgt beim Auslösen des Alarms automatisch eine **Alarmmeldung** an einen **externen Wachdienst**.

2.1.1.8 Externer Wachdienst

Der externe Wachdienst wird automatisch bei Alarmauslösung benachrichtigt und führt unmittelbar nach der Alarmauslösung eine Überprüfung **vor Ort** durch. Er informiert bei festgelegten Ereignissen oder einer unklaren Situation vor Ort unverzüglich die von der d.velop AG benannten Ansprechpartner.

2.1.1.9 Sicherheitszonen

Innerhalb der Firmengebäude der d.velop AG befinden sich einzelne Sicherheitsbereiche. Diese Sicherheitsbereiche sind durch eine **zweite Zutrittskontrolle** abgesichert. Die Sicherheitszonen sind für Außenstehende nicht erkenntlich und werden nur in einem internen Dokument zur IT Sicherheit der d.velop AG aufgeführt. Die **Sicherheitsbereiche** umfassen unter anderem die Serverräume, die Räume von Geschäftsführung, HR und IT-Administration sowie den Raum für die Aufbewahrung der Fernwartungs-Token.

2.1.1.10 Besucherausweise / Besucherregelung

Besucher der d.velop AG werden im Zentralgebäude empfangen. Außerhalb der Geschäftszeiten ist das Zentralgebäude verschlossen und ein Zutritt ist ausschließlich mit einem personalisierten Mitarbeiterausweis möglich. Der Empfang der d.velop AG registriert die Besucher und händigt allen Besuchern einen Besucherausweis aus. Zutritt zu anderen Gebäuden als dem Zentralgebäude wird Besuchern nicht gewährt. Ein selbständiges Bewegen von Besuchern in den anderen drei Gebäuden ist ausgeschlossen.

2.1.2 Zugangskontrolle

2.1.2.1 Benutzername & Kennwort

Die d.velop AG betreibt eine **Microsoft Windows Domäne** mit Microsoft Windows Rechnern. Der Zugang zu den einzelnen Rechnern wird über eine Windows Anmeldung gesteuert. Für die Anmeldung sind ein Benutzername und ein Kennwort erforderlich. Die Vergabe von Benutzernamen erfolgt für Mitarbeiter ausschließlich personalisiert.

2.1.2.2 Kennwortrichtlinie

In der Richtlinie für *Mitarbeiter-Kennwörter* wird vorgegeben, wie ein Kennwort aufgebaut sein muss. Diese Kennwortrichtlinie gilt für alle IT Systeme. Aufgrund der Tatsache, dass nicht alle IT Systeme eine automatische Überwachung einer Kennwortrichtlinie unterstützt, liegt ein Schwerpunkt in dem Zugang zu unseren Windows Rechnern. Die Kennwortrichtlinie für die Windows Domäne macht die folgenden Vorgaben:

Vorgaben für das Windows Domänen Kennwort

- Es muss Zeichen aus mindestens drei der folgenden Kategorien enthalten:
    - Großbuchstaben
    - Kleinbuchstaben
    - Zahlen
    - Sonderzeichen (z.B. ; / ? ! # *)
- Maximales Kennwortalter: 100 Tage
- Minimale Kennwortgültigkeit: 1 Tag
- Minimale Kennwortlänge: 8 Zeichen
- Kennwortzyklus (bevor das ursprüngliche wieder genutzt werden kann): 6 Kennwörter
- Konto sperren nach definierter Anzahl Fehlversuche, zunächst temporär, dann dauerhaft

- Besonderheit für Administratoren:
    - Kennwort muss Zeichen aus allen vier oben genannten Kategorien enthalten
    - Minimale Kennwortlänge: 12 Zeichen

Diese Vorgaben werden automatisch überwacht. 14 Tage vor Ablauf des Kennwortalters werden die Mitarbeiter dazu aufgefordert Ihr Kennwort zu ändern. Erfolgt nach mehrmaliger automatisierter Aufforderung keine Kennwortänderung, muss das Kennwort nach Ablauf zwingend bei der nächsten Systemanmeldung geändert werden.

2.1.2.3 Autorisierungsprozess für Zugangsberechtigungen

Zugangsberechtigungen zu IT-Systemen der d.velop AG werden ausschließlich personalisiert vergeben. Die Vergabe erfolgt für Mitarbeiter durch einen geregelten Workflow, welcher durch die HR-Abteilung bei dem Eintritt ins Unternehmen gestartet wird. Die Anfrage auf Erteilung einer Zugangsberechtigung wird **immer** an den direkten Vorgesetzten und die IT-Abteilung geleitet. Der Vorgesetzte entscheidet über die Annahme und die Ablehnung des Antrags. Sonderberechtigungen werden ausschließlich nach vorheriger Zustimmung der Unternehmensleitung eingeräumt.

2.1.2.4 Single-Sign-On

Wenn interne IT Systeme ein Single-Sign-On unterstützen, wird dieser Mechanismus genutzt. Für Systeme ohne einen solchen Mechanismus gilt die Kennwortrichtlinie ohne die Ergänzungen zu den zeitlichen Aspekten.

2.1.2.5 Bildschirmschoner mit Kennwortschutz

Bei Abwesenheit eines Mitarbeiters von seinem Arbeitsplatz wird ein Bildschirmschoner mit Kennwortschutz aktiviert. Der Bildschirmschoner mit Kennwortschutz wird spätestens nach **15 Minuten** automatisch aktiviert. Die Mitarbeiter sind organisatorisch über eine Richtlinie angewiesen, unabhängig hiervon den Bildschirm beim Verlassen des Arbeitsplatzes immer sofort zu sperren.

2.1.2.6 Unternehmensweite Virenschutzlösung

Zum Schutz vor Schadsoftware wird eine unternehmensweite Virenschutzlösung verwendet. Die Aktualisierung der Virensignaturen erfolgt automatisiert. Auf allen betrieblichen Geräten (Server, PC, Notebooks) ist dieser Virenschutz eingerichtet und aktiviert.

2.1.2.7 Unternehmensweite Spamschutzlösung

Zum Schutz vor unerwünschten E-Mails und somit auch zum Schutz vor Viren und Trojanern ist eine unternehmensweite Spamschutzlösung installiert. Für alle eingehenden E-Mails wird automatisiert eine Spam-Überprüfung vorgenommen.

2.1.2.8 Firewall Systeme

Zum Schutz vor ein unerwünschtes Eindringen in die Firmennetzwerke der d.velop AG ist ein Firewall System installiert und konfiguriert.

2.1.3 Zugriffskontrolle

Der **Zugriff** auf die IT Systeme der d.velop AG erfolgt ausschließlich **bedarfsorientiert** und nach dem „Need to know Prinzip". Die Mitarbeiter der d.velop AG erhalten nur Zugriff auf die IT Systeme, welche für die Erfüllung der täglichen Arbeit unbedingt notwendig sind.

2.1.3.1 Verwaltung und Vergabe von Berechtigungen

Bei Anwendungen und Systemen, die ein detailliertes **Berechtigungskonzept** mit Rollen oder Berechtigungsprofilen unterstützen, wird der Zugriff über ein Berechtigungskonzept innerhalb der Software eingeschränkt. Auch hierbei erhalten nur die Personengruppen Zugriff auf Anwendungen und Systeme, welche zur Aufgabenerfüllung unbedingt notwendig sind.

Zugriffsberechtigungen auf Netzwerkebene, wie beispielsweise Netzwerklaufwerke, Computer und Drucker, werden über ein Berechtigungskonzept auf Betriebssystemebene vergeben. Die Vergabe dieser Berechtigungen wird über eine Verfahrensanweisung gesteuert.

Die Vergabe von zusätzlichen Zugriffsberechtigungen erfolgt über einen Workflow, welcher durch den Mitarbeiter als auch durch die IT-Abteilung gestartet werden kann. Der Prozess erfasst dabei die gewünschte Berechtigung und wird anschließend sowohl dem Vorgesetzten als auch der IT-Abteilung zur Prüfung und Freigabe vorgelegt. Sonderberechtigungen werden ausschließlich nach vorheriger Zustimmung der Unternehmensleitung eingeräumt.

2.1.3.2 Akten- und Datenträgervernichtung

Die d.velop AG hat in ausgewiesenen Bereichen Datenschutztonnen aufgestellt. Diese Stahlcontainer sind ständig verschlossen und dienen der Sammlung von zu vernichtenden Unterlagen und Datenträgern. Die Entsorgung wird von zertifizierten Unternehmen datenschutzkonform durchgeführt. Die Vernichtung der über die Datenschutztonnen entsorgten Dokumente erfolgt über Maschinen, welche gemäß DIN 66399 arbeiten.

2.1.4 Trennungskontrolle

Innerhalb der d.velop AG werden unterschiedliche, **physikalisch getrennte IT Systeme** verwendet. Für die physikalische Speicherung von Daten werden logisch getrennte Datenbanken eingesetzt. Jede Datenbank verfügt über zweckgebundene Zugriffsberechtigungen.

2.1.4.1 Trennung von Entwicklungs-, Test- und Produktivumgebung

Die IT-Systeme der d.velop AG sind in Entwicklungs-, Test- und Produktivumgebung unterteilt. Der Zugriff zu den einzelnen Umgebungen ist mit bedarfsgerechten Zugriffsberechtigungen versehen. Das Einspielen von neuen Programmversionen erfolgt grundsätzlich in einem mehrstufigen Prozess, bei welchem zuerst Testumgebungen zur Funktionsprüfung verwendet werden.

2.1.4.2 Verwendung von Testdaten

Innerhalb von Entwicklung- und Testumgebungen werden ausschließlich anonyme oder anonymisierte Testdaten verwendet. Von einem Zugriff auf Produktivdaten wird grundsätzlich abgesehen. Entsprechende Berechtigungskonzepte verhindern den Zugriff auf Produktivdaten durch unautorisierte Mitarbeiter.

2.1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Eine Pseudonymisierung von Daten erfolgt unmittelbar bei der Verarbeitung, wenn anstelle des Namens einer betroffenen Person die Daten ausschließlich unter einer Kennziffer oder einem anderen Kennzeichen verarbeitet werden (z.B. Personalnummer oder User-ID). Zudem sind für sämtliche Prozesse entsprechende Löschkonzepte implementiert, welche die Löschung nicht mehr benötigter Daten nach einer angemessenen Zeit realisieren.

2.1.6 Homeoffice und mobiles Arbeiten

Homeoffice und mobiles Arbeiten sind ausschließlich gemäß den Vorgaben in der IT-Richtlinie zulässig. Dabei ist insbesondere sicherzustellen, dass der Arbeitsplatz den Vetraulichkeitsanforderungen der d.velop AG entspricht. Besondere Anforderungen oder Verbote von Auftraggebern werden beachtet.

2.2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.2.1 Weitergabekontrolle

Der Transport von Sicherungsbändern in andere Brandabschnitte außerhalb der Firmengebäude wird durch mindestens zwei Mitarbeiter der d.velop AG begleitet. Für den Transport von Daten auf elektronischen Weg werden Notebooks mit einer auf Betriebssystemebene integrierten **Festplattenverschlüsselung** (*Bitlocker*) verwendet. Dieses Verfahren wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als sicher bewertet.

2.2.1.1 Verschlüsselung von Datenträgern

Datenträger mobiler Endgeräte (Notebooks, Smartphones, Tablets) sowie externe Datenträger sind verschlüsselt. Die Verschlüsselung wird mithilfe von im Betriebssystem integrierten Verschlüsselungsverfahren (Microsoft BitLocker, Apple iOS-Verschlüsselung) realisiert.

2.2.1.2 Verschlüsselung von Funk-Netzwerken

Sämtliche der auf dem d.velop campus ausgestrahlten Funk-Netzwerke (WLAN), welche interne Systeme der d.velop AG erreichen, kommunizieren ausschließlich verschlüsselt. Die Netzwerke sind für unterschiedliche Interessengruppen (Mitarbeiter, Schulungsteilnehmer) aufgeteilt und nutzen als Sicherheitsstandard WPA2. Neben den verschlüsselten Funk-Netzwerken gibt es zusätzlich ein unverschlüsseltes und öffentlich zugängliches Netzwerk. Aus dem öffentlich zugänglichen Netzwerk und dem Schulungsteilnehmer-Netzwerk ist ein Zugriff auf interne Bereiche der d.velop AG nicht möglich.

2.2.1.3 Gesicherter File Transfer oder sonstiger Datentransport

Die d.velop AG betreibt extern erreichbare IT-Systeme. Sofern die genutzten Dienste eine Verschlüsselung des Datentransports ermöglichen (HTTPS, SSL/TLS) ist diese konfiguriert und als bevorzugte Kommunikationsmöglichkeit definiert. Kritische Dienste (VPN, Filetransfer von Support- und Anwendungsdaten) sind ausschließlich über verschlüsselte Kommunikationswege erreichbar.

2.2.2 Eingabekontrolle

In einigen Bereichen wird Software eingesetzt, welche ein Audit-Log über sämtliche Eingaben führt und anhand dessen nachvollzogen werden kann, welche Eingaben oder Änderungen von welcher Person vorgenommen worden sind. Bei Software, welche diese Mechanismen nicht unterstützt, wird über Verfahrensanweisungen das Verarbeiten der Daten festgelegt.

2.2.2.1 Dokumenten Management System (DMS)

Die Mitarbeiter der d.velop AG sind per Richtlinie dazu angehalten, aufbewahrungs- und somit archivierungspflichtige Dokumente im von der d.velop AG hergestellten DMS-System zu archivieren. Dazu zählen Aufzeichnungen und elektronischen Daten, die notwendig sind, um Ordnungsmäßigkeit und Nachvollziehbarkeit sämtlicher Unternehmensprozesse sicherzustellen. Das DMS-System ermöglicht dabei Änderungshistorien sowie eine revisionssichere Archivierung der gespeicherten Daten.

2.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Einer zufälligen Zerstörung oder dem Verlust von Daten begegnet die d.velop AG durch eine Vielzahl von Maßnahmen. **Firewall-Lösungen** verhindern ein Eindringen in das Firmennetzwerk über das öffentliche Netz und sichern interne Netzsegmente vor unberechtigten Zugriffen. Eine unternehmensweite, einheitliche **Viren- und Spamschutzlösung** beugt dem Eindringen von Schadsoftware vor.

Die Ausfallsicherheit unserer Systeme unterstützt hierbei die Verfügbarkeit **Ihrer** Systeme. Häufig kann nur der Support der d.velop AG eine schnelle Lösung eines Problems herbeiführen, so des es bei Ihnen erst gar nicht zu einem Beschränkung der Verfügbarkeit oder gar dem Ausfall von Systemen kommt.

2.3.1 Notfallplan

Im Notfallhandbuch der d.velop AG sind die konkreten Handlungsanweisungen dokumentiert, welche im Falle eines Notfalls abgearbeitet werden müssen. Hier werden Notfälle wie „*Zerstörung des gesamten d.velop Campus*“, „Brand“, „Wassereinbruch“, „*Ausfall der Klimaanlage (Anstieg der Temperatur)*“, „Ausfall der Klimaanlage“, „*Stromausfall/ Spannungsschwankungen*“, „*Ausfall der Telefon- / Internetleitung*“ und der „*Hardwareversagen*“ behandelt. Regelmäßig durchgeführte und protokollierte Notfallübungen gewährleisten, dass die entwickelten Konzepte im Not-/ Katastrophenfall korrekt definiert sind und funktionieren.

2.3.2 Bereitschaftsdienst

Sollte es zu Verfügbarkeitsproblemen kommen, steht allen Mitarbeitern der d.velop AG ein Bereitschaftsdienst zur Verfügung. Der Bereitschaftsdienst der d.velop AG ist dazu auch an Sonn- und Feiertagen erreichbar.

2.3.3 Sicherungskonzept

Die Daten und IT-Systeme der d.velop AG werden über mehrstufige Backupkonzepte gesichert. Die Häufigkeit und Dauer der Aufbewahrung beziehen sich dabei auf die Sensibilität der gesicherten Daten. Die für die Hardware verwendete Sicherung befindet sich in einem anderen Brandabschnitt als das Rechenzentrum. Die Aufbewahrung der Sicherungen erfolgt unter anderen in einem brandgeschützten Safe, als auch in einem vom d.velop campus entfernen Schließfach. Der Safe befindet sich dabei wiederum in einem anderen Brandabschnitt als das Rechenzentrum und der Standort der Sicherungshardware.

2.3.4 Einspielen von Sicherheitsupdates

Sicherheitsupdates werden für produktive Endgeräte zeitnah nach dem Erscheinen eingespielt. Vorgelagerte Tests gewährleisten, dass die Updates problemlos eingespielt werden können. Sämtliche produktive Server werden regelmäßig in geplanten Wartungsfenstern aktualisiert. Im Falle von außerplanmäßig bekanntgewordenen kritischen Sicherheitslücken erfolgt ein umgehendes Einspielen entsprechender Patches.

2.3.5 Redundante Rechenzentrums-Hardware

Die d.velop AG betreibt die wichtigsten Systeme zur Aufrechterhaltung des Betriebs **redundant**, sodass ein ausfallfreier Betrieb gewährleistet werden kann. Zudem erfolgt die Spiegelung von Backups in einen weiteren Brandabschnitt.

2.3.6 Überwachung der IT-Systeme

Die d.velop AG verfügt über verschiedene Monitoring- und Alarmierungssysteme, welche die IT-Abteilung während der Geschäftszeiten und den Bereitschaftsdienst in dringenden Fällen rund um die Uhr über Abweichungen vom Normalbetrieb unverzüglich informieren. Dies ermöglicht eine sofortige Erkennung von Fehlverhalten und eine verkürzte Zeit zur Wiederherstellung des Normalbetriebs.

2.3.7 Schwachstellen- und Belastbarkeitstests

Die d.velop AG führt regelmäßig interne und extern beauftragte Schwachstellen- und Belastbarkeitstests durch. Diese gewährleisten, dass Schwachstellen oder andere Defizite rechtzeitig festgestellt und behoben werden.

2.3.8 Technische Überwachung des Rechenzentrums

Das Rechenzentrum der d.velop AG ist mit verschiedenen Messtechniken zur frühzeitigen Erkennung von möglicherweise eintretenden Elementarschäden ausgestattet. Die Messtechniken kontrollieren unter anderem die Temperatur und Luftfeuchtigkeit, sowie die aktuelle Netzspannung als auch ein mögliches Wassereindringen in die Räume. Rauchansaugsysteme kontrollieren zudem stetig die Luft und melden bereits frühe Stände von möglichen Schwelbränden. Alle Systeme sind mit den Monitoringsystemen der d.velop AG verbunden und alarmieren die IT-Abteilung und den Bereitschaftsdienst bei Abweichungen vom Normalbetrieb.

2.3.9 Stromversorgung des Rechenzentrums

Das Rechenzentrum der d.velop AG verfügt über unterbrechungsfreie Stromversorgungs-Systeme (USV). Die USV fangen Spannungsschwankungen des Stromnetzes ab. Im Falle eines Stromausfalls gewährleisten die Batterien der USV ein kontrolliertes Herunterfahren aller Systeme. Datenverluste und Folgeschäden an der Rechenzentrumshardware können somit verhindert werden.

2.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

2.4.1 Datenschutz-Management

Die d.velop AG verfügt über ein Datenschutzmanagementkonzept mit klar definierten Verantwortlichkeiten und Arbeitsabläufen. Ein regelmäßig sich treffendes Statusteam erörtert fortlaufend alle für den Datenschutz und die Informationssicherheit erforderlichen Maßnahmen und Entwicklungen. Es kontrolliert auch die Umsetzung der Maßnahmen in der d.velop AG und weist den Vorstand auf notwendige oder sinnvolle Veränderungen hin.

2.4.1.1 Datenschutzleitbild

Für die d.velop AG sind der Schutz der Persönlichkeitsrechte und der Datenschutz von größter Bedeutung. Diesem Schutzbedarf begegnet die d.velop AG mit einem unternehmensweiten Datenschutzmanagement. Das Datenschutzmanagement der d.velop AG orientiert sich an den IT-Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), an den Empfehlungen der Gesellschaft für Datenschutz und Datensicherung e.V. (GDD) sowie an den Empfehlungen des bitkom als dem übergreifenden Branchenverband. Es wird regelmäßig oder anlassbezogen überprüft und aktualisiert.

2.4.1.2 Datenschutz-Richtlinie

Die d.velop AG hat durch den Vorstand eine unternehmensweite Richtlinie verabschiedet, aus der sich die Bedeutung von Datenschutz und Informationssicherheit für die gesamte d.velop-Gruppe ergibt. Diese Richtlinie ist Grundlage der von der d.velop AG getroffenen und u.a. in diesem Dokument dokumentierten Maßnahmen und implementierten Geschäftsprozessen zum Datenschutz.

2.4.1.3 Benennung eines Datenschutzbeauftragten

Die d.velop AG hat zum **1. Januar 2013** einen **externen Datenschutzbeauftragten schriftlich benannt**. Der externe betriebliche Datenschutzbeauftragte der d.velop AG ist Herr Rechtsanwalt Sascha Kremer. Sascha Kremer ist vom TÜV Rheinland zertifizierter externer Datenschutzbeauftragter, Datenschutzauditor und Fachanwalt für Informationstechnologie-Recht. ER bildet selbst regelmäßig Datenschutzbeauftragte (intern/extern) aus und veröffentlicht fortlaufend in Fachzeitschriften zum Datenschutzrecht und zur Datensicherheit.

Die Kontaktdaten des Datenschutzbeauftragten lauten:

Sascha Kremer
Fachanwalt für IT-Recht
zertifizierter Datenschutzbeauftragter und Datenschutzauditor
Brückenstraße 21, 50667 Köln (Innenstadt)
Telefon +49 (171) 8319621
E-Mai: datenschutz@d-velop.de

Der externe betriebliche Datenschutzbeauftragte der d.velop AG ist direkt dem **Vorstandsvorsitzenden** der d.velop AG unterstellt und somit gemäß Art. 38 Abs. 3 DS-GVO in Ausübung seiner Tätigkeit auf dem Gebiet des Datenschutzes weisungsfrei.

2.4.1.4 Fachkunde des externen Datenschutzbeauftragten

Der externe Datenschutzbeauftragte der d.velop AG hat die erforderliche Fachkunde zum Ausüben der Tätigkeit des betrieblichen Datenschutzbeauftragten. Er ist Autor u.a. des Standardwerkes zur DSGVO „Laue/Kremer: Das neue Datenschutzrecht in der betrieblichen Praxis“ (Nomos Verlag, 2. Auflage 2019) und der Kommentierung der Art. 24,

26, 27, 28 und 29 DSGVO im Heidelberger Kommentar zur DSGVO (2. Auflage 2020). Der folgende Ausbildungs- und Fortbildungsnachweis führt weitere Nachweise auf:

Rechtsanwalt
Seit 2006

Fachanwalt für Informationstechnologie-Recht
Seit 2014

Externer Datenschutzbeauftragter (TÜV)
TÜV Rheinland Akademie GmbH
Abschluss Februar 2013 (Zertifikats-Nr. 1992690)

ARGE Betrieblicher Datenschutz
DataKontext Verlag
2 Termine jährlich seit 2015, durchgeführt durch Sascha Kremer als Leiter der ARGE

Seminar Löschen nach DSGVO
DataKontext Verlag
2 Termine jährlich seit 2017, durchgeführt durch Sascha Kremer als Leiter des Seminars (gemeinsam mit Informatiker Dr. Stiemerling)

Seminar Datenschutzverletzungen
DataKontext Verlag
2 Termine jährlich seit 2019, durchgeführt durch Sascha Kremer als Leiter des Seminars

2.4.1.5 Berichtswesen

Der externe Datenschutzbeauftragte berichtet **direkt** an den **Vorstandsvorsitzenden** der d.velop AG. Zu diesem Zweck finden **zweiwöchentlich Status-Meetings** statt, an denen auch der IT-Sicherheitsbeauftragte, die IT-Leiterin und der Qualitätsbeauftragte der d.velop AG teilnehmen.

Weiterhin hat der externe Datenschutzbeauftragte **jederzeit** die Möglichkeit direkt den Vorstandsvorsitzenden anzusprechen. Neben den Statusmeetings werden Berichte und Anfragen direkt per E-Mail kommuniziert. Weiterhin werden wesentliche Entscheidungen in einem Tätigkeitsbericht des externen Datenschutzbeauftragten festgehalten.

2.4.1.6 Tätigkeitsberichte

Der externe Datenschutzbeauftragte führt Tätigkeitsberichte. In diesen Tätigkeitsberichten werden die einzelnen Aktivitäten und Vorkommnisse rund um das Thema Datenschutz festgehalten. Dieser Tätigkeitsbericht dient weiterhin zur Vorlage beim Vorstandsvorsitzendem (Berichtswesen). Die Tätigkeitsberichte sind vertraulich und nur für den externen Datenschutzbeauftragten und den Vorstandsvorsitzenden bestimmt.

2.4.1.7 Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGV)

Das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO für die eigenen Verarbeitungen der d.velop AG und das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO für die von der d.velop als Auftragsverarbeiter (z.B. bei d.velop Cloud) durchgeführten Verarbeitungen werden entsprechend den gesetzlichen Vorgaben von der d.velop AG geführt. Hierfür greift die d.velop AG auf das von ihr selbst mit

Unterstützung u.a. des externen Datenschutzbeauftragten entwickelte, eigene Produkt „GDPR Compliance Center" zurück, welches auf dem d.3 System der d.velop AG basiert.

2.4.1.8 Qualitätsmanagementbeauftragter

Die d.velop AG hat einen Qualitätsmanagementbeauftragten (QMB) benannt, welcher für das **Qualitätsmanagementsystem** der d.velop AG verantwortlich ist. Dieses Qualitätsmanagementsystem enthält eine Vielzahl von Arbeitsanweisungen, Verfahrensanweisungen, Richtlinien und Merkblätter, welche für das Datenschutzmanagement der d.velop AG verbindlich sind. Der Qualitätsmanagementbeauftragten ist in Bezug auf die Belange des Qualitätsmanagementsystems direkt dem Vorstandsvorsitzenden der d.velop AG unterstellt.

2.4.1.9 IT-Sicherheits- und Datenschutzteam

Die d.velop AG hat ein IT-Sicherheits- und Datenschutzteam, welches aus dem externen Datenschutzbeauftragten, dem Qualitätsmanagementbeauftragten, dem IT-Sicherheitsbeauftragten, der Leitung der IT Abteilung, dem externen Head of Legal und dem Vorstandsvorsitzenden der d.velop AG besteht. Es trifft sich regelmäßig alle zwei Wochen.

2.4.1.10 Verpflichtung der Mitarbeiter

Alle Mitarbeiter der d.velop AG werden schriftlich auf die Vertraulichkeit (früher: das **Datengeheimnis** gemäß § 5 BDSG), das **Sozialgeheimnis** (§ 35 SGB I), auf die **Wahrung von Geschäftsgeheimnissen** (§ 17 UWG) sowie bei Bedarf auf das Fernmeldegeheimnis (§ 88 TKG) und das Bankgeheimnis verpflichtet. Diese Verpflichtungserklärung ist fester Bestandteil des Arbeitsvertrages und Teil der Personalakte eines Mitarbeiters. Der Verpflichtungserklärung ist ein **Merkblatt** beigefügt, in welchem die Bedeutung dieser einzelnen Paragraphen erläutert wird.

2.4.1.11 Schulungsmaßnahmen

Die Datenschutzunterweisung ist Bestandteil des Einstellungsverfahrens für neue Mitarbeiter der d.velop AG. Im Rahmen dieses Einstellungsverfahrens findet sowohl eine Unterweisung bezüglich des Datenschutzes gemäß **DS-GVO** statt als auch eine Unterweisung bezüglich des Sozialgeheimnisses (**SGB**). Neben diesen Präsenzschulungen werden aktuelle Themen rund um den Datenschutz über das Intranet und das Datenschutzportal der d.velop AG an die Mitarbeiter herangetragen. Die interne E-Mail Adresse datenschutz@d-velop.de steht zudem allen Mitarbeitern zur Verfügung, um Fragen und Datenschutzvorfälle an den externen betrieblichen Datenschutzbeauftragen zu richten. Zudem erfolgen alle zwei bis drei Jahre Präsenzschulungen für alle Mitarbeiter der d.velop AG, jährliche Schulungen für Auszubildende und bei Bedarf spezielle Schulungen für bestimmte Fachbereiche (z.B. IT, HR).

2.4.1.12 Intranet und Datenschutzportal

Aktuelle Neuigkeiten und Änderungen bezogen auf den Datenschutz und die IT Sicherheit der d.velop AG werden sowohl in **Mitarbeiterversammlungen** als auch im **Intranet** der d.velop AG veröffentlicht. Jeder Mitarbeiter der d.velop AG hat die Verpflichtung, einmal täglich die Plattform zu „besuchen". Über das Intranet hat der Mitarbeiter Zugriff auf alle relevanten Dokumente zum Datenschutz.

Ein gesonderter Bereich im Intranet ist das Datenschutzportal. Über dieses Datenschutzportal hat jeder Mitarbeiter die Möglichkeit, die in den Datenschutzunterweisungen verwenden Präsentationen nochmals einzusehen, aktiv

Fragen zu stellen oder eine FAQ zu Datenschutzthemen aufzurufen. Das Datenschutzportal ist **innerhalb des Firmennetzwerkes** der d.velop AG unter der Adresse „**datenschutz.d-velop.de**" erreichbar.

2.4.2 Management bei Datenschutzverletzungen

Beim Verdacht auf eine Datenschutzverletzung gibt es einen in der d.velop AG festgelegten und beschriebenen Informationslauf, der gewährleistet, dass durch das IT-Sicherheits- und Datenschutzteam unverzüglich der Sachverhalt geprüft werden kann. Soweit erforderlich werden vom IT-Sicherheits- und Datenschutzteam die notwendigen Gegenmaßnahmen eingeleitet und entsprechend den gesetzlichen Verpflichtungen die Aufsichtsbehörden und ggf. auch die betroffenen Personen informiert. Im Anschluss erfolgt eine umfängliche Bewertung des Vorgangs, um hieraus die „lessons learned" abzuleiten und ggf. systematische oder punktuelle Veränderungen zur Vermeidung zukünftiger Datenschutzverletzungen vorzunehmen.

2.4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Die von der d.velop AG genutzten Systeme werden stets datenschutzfreundlich vorkonfiguriert ausgeliefert und intern bereitgestellt. Verarbeitungen, die nicht erforderlich sind, werden nur auf Veranlassung des Anwenders oder nach einer vorherigen Einwilligung vorgenommen. Optionale Eingabefelder in Anwendungen der d.velop AG sind als solche gekennzeichnet, eine Verpflichtung zum Ausfüllen besteht selbstverständlich nicht.

2.4.4 Auftragskontrolle

Die **d.velop AG als Auftragnehmer** unterliegt bei der Auftragsverarbeitung dem **Art. 28 DSGVO** oder dem **§ 80 SGB X**. Hierbei ist der **Auftraggeber** als Verantwortlicher für die Einhaltung der datenschutzrechtlichen Vorschriften und Gesetze verantwortlich. Diese Verantwortung des Auftraggebers unterstützt die d.velop AG aktiv durch eine Vielzahl von technischen und organisatorischen Datenschutzmaßnahmen innerhalb der d.velop AG. Das Ihnen vorliegende Dokument ist Bestandteil dieser Datenschutzmaßnahmen. Soweit erforderlich schließt die d.velop AG mit Ihnen als Kunde einen den gesetzlichen Anforderungen entsprechenden Vertrag zur Auftragsverarbeitung ab.

2.4.4.1 Unterauftragnehmer

Die d.velop Gruppe ist ein Verbund von Unternehmen, bestehend aus der d.velop AG und mehreren **Tochtergesellschaften** der d.velop AG.

Die Tochtergesellschaften der d.velop AG sind spezialisiert auf Teilgebiete im ECM Umfeld und werden regelmäßig als Unterauftragnehmer zur Auftragsabwicklung herangezogen. Neben entsprechenden Gesellschafterverträgen und Dienstleistungsrahmenverträgen bildet die **Vereinbarung über die Auftragsverarbeitung** mit jeder Tochtergesellschaft einen wesentlichen Bestandteil der Auftragsverarbeitung. Über diese Vereinbarung über die Auftragsdatenverarbeitung wird der d.velop AG als **Hauptauftraggeber** immer ein *Kontrollrecht*, *Besichtigungsrecht* und *Weisungsrecht* eingeräumt.

In dem mit einem Kunden abgeschlossenen Vertrag zur Auftragsverarbeitung führt die d.velop AG die als Unterauftragnehmer eingesetzten Tochtergesellschaften sowie ggf. zusätzlich als Unterauftragnehmer eingesetzte, von der d.velop sorgfältig nach ihrer Eignung ausgewählte Dritte mit den von diesen jeweils erbrachten Leistungen auf. Mit Unterzeichnung des Vertrags oder ggf. separat stimmt der Kunde dann der Unterbeauftragung zu. Selbstverständlich stehen dem Kunden bei den Unterauftragnehmern ebenfalls die vereinbarten Kontrolle-, Besichtigungs- und Weisungsrechte rechte zu.

Die d.velop AG und ihre Unterauftragnehmer werden regelmäßig durch Kunden oder externe Dritte (z.B. Prüfgesellschaften) auditiert. Etwaige bei den Audits ausgesprochene Empfehlungen werden im Nachgang vom IT-Sicherheits- und Datenschutzteam der d.velop AG bewertet und hiernach durch die d.velop AG umgesetzt, wo erforderlich oder zur Verbesserung des Datenschutzes sinnvoll.

Sämtliche Leistungsbeziehungen der d.velop AG zu ihren Kunden und Unterauftragnehmern werden von der d.velop AG in ihrem eigenen DMS-System dokumentiert und transparent gemacht. So ist jederzeit feststellbar, für wen die d.velop AG mit welchen Unterauftragnehmern welche Leistungen erbringt.

3 Besondere Schutzmaßnahmen für d.velop OnPremise Installationen

Die nachfolgend beschriebenen Maßnahmen gelten für d.velop OnPremise Installationen. Abhängig von den Vorgaben des Auftraggebers sind für die Wartung und Pflege verschiedene Maßnahmen möglich.

3.1 Zugang zu OnPremise Installationen (Fernwartung)

Gängige Verfahren sind

a) die telefonische Anfrage vor der Fernwartung mit anschließender, expliziter Freischaltung der Fernwartungszugänge mit entsprechender Protokollierung,
b) die Verwendung von "Hardware Tokens" (z.B. RSA) für den Zugang zu den IT Systemen des Kunden über eine Fernwartungssoftware (diese werden stets in der Sicherheitszone beim Support aufbewahrt, siehe Zutrittskontrolle), oder
c) die Verwendung einer VPN Software (Cisco, CheckPoint u.a.) mit anschließender Remote Sitzung (Remote Desktop).

Die d.velop AG verwendet im Standard die Anwendung ***TeamViewer***. Bei allen Verfahren wird der Zugang zu den Systemen des Auftraggebers durch den Auftraggeber selbst kontrolliert und nach Maßgabe des Hauptvertrags durch die d.velop AG protokolliert (siehe unten Eingabekontrolle).

3.2 Zugriff auf OnPremise Installationen (Fernwartung)

Der Auftraggeber kann

a) den Zugriff über entsprechende Benutzerkonten auf Betriebssystemebene in seiner IT Umgebung einschränken,
b) innerhalb von d.3 explizite Fernwartung-Accounts (Benutzer) einrichten. Über das detaillierte Berechtigungskonzept in d.3 kann der Auftraggeber den Zugriff auf die Daten innerhalb des d.3 Archivs granular fein steuern, oder
c) den Zugriff im Beisein begleiten und die Ausführung der getätigten Aktionen überwachen.

3.3 Integrität von Fernwartungen

Das verwendete Verfahren zur Fernwartung muss eine Verschlüsselung auf Leitungsebene (HTTPS, SSL, TLS, IPSEC) unterstützen.

Ergänzend empfiehlt die d.velop dem Auftraggeber die Anonymisierung der bei der Fernwartung zugänglichen personenbezogenen Daten. Nicht anonymisierte Dokumente (Screenshots, Log-Files u.ä.) werden von der d.velop nicht entgegengenommen, wenn diese besondere Kategorien personenbezogener Daten oder Sozialdaten enthalten.

3.4 Eingabekontrolle von Fernwartungen

Abhängig von den Vorgaben des Auftraggebers sind verschiedene Verfahren möglich.

Die Arbeiten werden auf Systemen des Auftraggebers ausgeführt, sodass dieser für die Protokollierung der Eingaben verantwortlich zeichnet.

In d.3 kann ein Benutzerkonto eingerichtet werden (siehe oben Zugriff), welches die Protokollierung sämtlicher Zugriffe durch die d.velop ermöglicht.

Angaben zu Fernwartungszugriffen werden nach Maßgabe des Hauptvertrags durch die d.velop im Ticketsystem zu dem einzelnen Auftraggeber mit Angaben zu Zeitpunkt, Dauer, Beteiligten, Art des Zugangs, Grund, Ergebnisse und ggf. erfolgten Eingaben/Änderungen sowie etwaigen Folgeaufgaben protokolliert.

4 Besondere Schutzmaßnahmen für die von d.velop angebotenen Cloud-Produkte

Die nachfolgend beschriebenen Maßnahmen gelten größtenteils für alle von d.velop angebotenen Cloud-Produkte (nachfolgend Cloud-Systeme). Besondere Schutzmaßnahmen, welche nur einzelne Cloud-Produktlinien betreffen sind als solche aufgeführt.

4.1 Vertraulichkeit

4.1.1 Zugangskontrolle

4.1.1.1 Persönlicher und individueller Login

Der Zugang zu Cloud-Systemen erfolgt mit personalisierten Accounts. Für die bereitgestellten Accounts gelten die Punkt 2.1.2 beschriebenen Sicherheitsmaßnahmen. Für die automatisierte Bereitstellung von Updates werden eingeschränkte Serviceaccounts verwendet.

4.1.1.2 Autorisierungsprozess für Zugangsberechtigungen zu Kundensystemen

Zugangsberechtigungen zu Cloud-Systemen werden ausschließlich nach dem Principle of least privilege vergeben. Die Vergabe erfolgt für Mitarbeiter durch einen geregelten und nachvollziehbaren Workflow über das interne Ticketsystem.

4.1.1.3 Zugang zu virtuellen Maschinen

Der Zugang zu Cloud-Systemen in Form von virtuellen Maschinen ist über ein mehrstufiges Zugangskonzept realisiert. Ein direkter Zugriff von Clients auf das IT-System ist nicht möglich. Für den Zugriff werden zusätzliche Systeme als Zwischenschritt verwendet, welche wiederum nach aktuellem Stand der Technik abgesichert sind. Nur über die abgesicherten Systeme ist ein personalisierter Zugriff auf produktive virtuelle Maschinen möglich. Der Kreis der zugriffsberechtigten Personen ist stark eingegrenzt.

4.1.1.4 Protokollierung des Zugangs

Es erfolgt eine dauerhafte Protokollierung von erfolgreichen und fehlgeschlagenen administrativen Zugangsversuchen zu Cloud-Systemen. Eine Auswertung der Protokolle erfolgt stichprobenartig und im Bedarfsfall.

4.1.1.5 Mehrfaktor-Authentifizierung

Innerhalb der Produktlinie „d.velop cloud“ wird für administrative Tätigkeiten und die damit verbundenen Benutzeraccounts eine Mehrfaktor-Authentifizierung verwendet, welche neben Benutzer- und Passwortkennung zusätzlich ein zweites Medium zwecks Zugang zu den IT-Systemen erfordert. Das Medium ist nur einem begrenzten Personenkreis zugänglich.

4.1.1.6 Firewall

Sämtliche Cloud-Systeme sind durch Firewall-Technologien gegen Eingriffe von außen abgeschirmt. Die Firewall-Konfiguration ist dem Schutzbedarf der zu verarbeitenden Daten angepasst. Die hinter der Firewall betriebenen IT-Systeme sind nur soweit von extern freigeschaltet, wie erforderlich (bspw. Port 443 für HTTPS-Freigabe der Frontendserver zur Kommunikation mit dem Kunden).

4.1.2 Zugriffskontrolle

4.1.2.1 Verwaltung und Vergabe von Berechtigungen

Der Zugriff auf Cloud-Systeme unterliegt einem detaillierten Berechtigungskonzept, welches mittels Rollenprofilen den Zugriff auf IT-Systeme und den darauf verarbeiten Daten stark einschränkt. Auch hierbei erhalten nur die Personengruppen Zugriff auf Anwendungen und Systeme, welche zur Aufgabenerfüllung unbedingt notwendig sind.

4.1.3 Trennungskontrolle

4.1.3.1 Mandantentrennung

Innerhalb der Cloud-Systeme bekommt jeder Mandant eine eigene technische Kennung. Ein Mandant ist dabei üblicherweise eine Firma mit mehreren Mitarbeitern. Die Mandantenkennung wird bei jedem Aufruf verifiziert, damit die Trennung der Daten zwischen den Mandanten sichergestellt ist.

4.1.3.2 Trennung von Entwicklungs- und Produktivumgebung

Alle Cloud-Systeme sind in Entwicklungs-, Test- und Produktivumgebungen unterteilt. Der Kreis zugriffsberechtigter Mitarbeiter auf Test- und Produktivumgebungen ist stark eingegrenzt und auf Personengruppen beschränkt, für welche einen Zugriff zur Aufgabenerfüllung unbedingt notwendig ist.

4.1.4 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Wo möglich werden bei der Verarbeitung personenbezogener Daten keine Klarnamen, sondern Pseudonyme verwendet, z.B. bei der Bezeichnung von Dokumenten, die in Cloud-Systemen abgelegt werden. Im Übrigen obliegt es dem Kunden als Anwender der Cloud-Systeme, die von ihm zur Verarbeitung offengelegten personenbezogenen Daten bei Bedarf zu pseudonymisieren.

4.2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

4.2.1 Weitergabekontrolle

4.2.1.1 Transportverschlüsselung

Die Cloud-Systeme sind in Microservices segmentiert. Die Kommunikation zwischen einzelnen Microservices geschieht ausschließlich verschlüsselt. Zudem erfolgt immer eine Transportverschlüsselung sämtlicher extern erreichbarer Schnittstellen. Die Verschlüsselung erfolgt gemäß dem aktuellen Stand der Technik.

4.2.1.2 Dateiverschlüsselung

Alle Daten und Inhalte, die in den Cloud-Systemen gespeichert und verarbeitet werden, werden nach aktuellem Industriestandard verschlüsselt abgelegt.

4.2.1.3 Protokollierung des Veränderns oder Entfernens von Daten

Die Produktlinie „d.velop cloud“ bietet eine standardmäßige Protokollierung beim Verändern und Entfernen von abgelegten Daten. Die Protokollierung erfolgt dabei immer auf Anwendungsebene und ist dem Endanwender jederzeit ersichtlich.

4.2.2 Eingabekontrolle

4.2.2.1 Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten

Die Cloud-Systeme sind in Microservices segmentiert. Die einzelnen Microservices stellen einzelne Funktionen der bereitgestellten Anwendungen zur Verfügung. Die Verantwortlichkeiten dieser Microservices sind klar definiert und damit verbundene Zugriffsrechte sind auf den jeweiligen verantwortlichen Personenkreis eingegrenzt.

4.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

4.3.1 Notfallplan

Für die Cloud-Systeme sind konkrete Handlungsanweisungen dokumentiert, welche im Falle eines Notfalls abzuarbeiten sind. Regelmäßig durchgeführte und protokollierte Notfallübungen gewährleisten, dass die entwickelten Konzepte im Not-/ Katastrophenfall korrekt definiert sind und funktionieren.

4.3.2 Redundanzen

Sämtliche Cloud-Systeme sind so ausgelegt, dass die wichtigsten Systeme zur Aufrechterhaltung des Betriebs redundant und bei Bedarf über verschiedene Rechenzentren verteilt sind. Ein ausfallfreier Betrieb kann somit gewährleistet werden.

4.3.3 Sicherungskonzept

Die Produktlinie „d.velop cloud“ hat ein Sicherungskonzept implementiert, welches im Bedarfsfall eine zeitnahe Wiederherstellung ausgefallener IT-Systeme und darauf gespeicherter Daten ermöglicht.

Im Produktbereich der digitalen Post ("d.velop post" bzw. weitere Bezeichnungen könnten die folgenden sein: „d.velop postbox“, „d.velop file sharing“, „d.velop documents light“, „foxdox“) erfolgt sämtliche Datenhaltung der Plattform mehrfach redundant, das heißt auf mehreren Datenträgern parallel. Die Plattform verwendet verlässliche Speichermedien, welche für eine Verfügbarkeit von über 99 Prozent ausgelegt sind.

4.3.4 Einspielen von Sicherheitsupdates

Sämtliche produktive Cloud-Systeme werden regelmäßig in geplanten Wartungsfenstern aktualisiert. Im Falle von außerplanmäßig bekanntgewordenen kritischen Sicherheitslücken erfolgt ein umgehendes Einspielen entsprechender Patches.

4.3.5 Changemanagement Prozess

d.velop hat einen Changemanagement Prozess etabliert, welcher für alle Cloud-Systeme verpflichtend ist. Sämtliche Änderungen an Cloud-Systemen werden dokumentiert und versioniert. Die Entwicklung und das Einspielen neuer

Funktionalitäten erfolgt dabei immer nach einem geregelten mehrstufigen Prozess, wobei Änderungen zunächst in Entwicklungs- und Testsystemen getestet werden. Ein Einspielen in produktive Umgebungen erfolgt erst nach einer internen Qualitätsfreigabe.

4.3.6 Überwachung der IT-Systeme

Alle Cloud-Systeme werden über verschiedene Monitoring- und Alarmierungssysteme überwacht, welche das Betriebsteam über Abweichungen vom Normalbetrieb unverzüglich informieren. Dies ermöglicht eine sofortige Erkennung von Fehlverhalten und eine verkürzte Zeit zur Wiederherstellung des Normalbetriebs.

4.3.7 Schwachstellen- und Belastbarkeitstests

Für alle Cloud-Systeme werden regelmäßig interne und extern beauftragte Schwachstellen- und Belastbarkeitstests durchgeführt. Diese gewährleisten, dass Schwachstellen oder andere Defizite rechtzeitig festgestellt und behoben werden.