d.velop

Technische und organisatorische Maßnahmen (Schutzkonzept für Informationssicherheit, Datenschutz und Geheimnisschutz) der d.velop-Gruppe

Inhalt

1 Änderungshistorie

Version	Datum	Bearbeiter	Bemerkung
1.0.0	29.03.2018	SOCH/SKRE	Neuerstellung gemäß DSGVO
1.0.1	14.03.2018	SOCH	Anpassung Gliederung
1.0.2	22.08.2018	SOCH	Anpassung Punkt „Verschlüsselung von Funk-Netzwerken“
1.0.3	06.06.2019	SOCH	Revision, Anpassung Titel auf „Anlage: Technische und organisatorische Maßnahmen (IT- und Datenschutz-Sicherheitskonzept)“
1.0.4	25.10.2019	SOCH	Revision, Anpassung Formatierung und Punkt 2.2.2 Kennwortrichtlinie
1.1.0	30.04.2020	SOCH	Revision, Neuformatierung, Unterteilung in besondere Schutzmaßnahmen für On Premises und d.velop Cloud, Aktualisierung Punkte unterhalb von 2.1.1, Erweiterung Titel um Firmennamen
1.1.1	06.05.2020	SOCH	Überführung Mandantentrennung in eigenen Punkt 4.1.3.1
1.1.2	20.07.2020	SOCH	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	Anpassung betroffener Produktbereich in Punkt 4.3.3, Ergänzung Punkt 4.3.5 Changemanagement Prozess
1.2.0	27.04.2021	SOCH	Aktualisierung, Erweiterung um Geheimnisschutz, Anpassung DSB
1.2.1	08.06.2021	SOCH	Erweiterung Punkt 2.1.6 Homeoffice und mobiles Arbeiten
1.2.2	21.10.2021	EWIN	Anpassung DSB
1.2.3	02.02.2022	EWIN	Überführung in die neue Vertragsvorlage
1.2.4	02.08.2022	EWIN	Punkt 2.1.4.3 Deep-Learning hinzugefügt
1.2.5	05.09.2022	EWIN	Sprachliche Anpassung
1.2.6	12.09.2022	EWIN	§ 88 TKG durch § 3 TTDSG ersetzt
1.2.7	06.11.2023	EWIN	Punkt 2.1.4.3 Deep-Learning entfernt
1.2.8	21.11.2023	EWIN	2.4.1.9 UWG = GeschGehG
1.3.0	22.03.2024	SOCH/SBEN/NMOE	Restrukturierung, Anpassung an aktuelle technische und organisatorische Maßnahmen

2 Informationssicherheit Management System

d.velop hat ein Information Security Management System implementiert welches ISO/IEC 27001 zertifiziert und TISAX geprüft ist. Der Geltungsbereich, entsprechenden Zertifikate und weitere Details können folgender Internetseite entnommen werden: https://www.d-velop.de/ueber-d-velop/zertifizierungen

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

Die Verarbeitung von Daten in d.velop internen IT-Systemen erfolgt zentral durch die d.velop AG in einem ISO 27001 zertifizierten Rechenzentrum.

Die Verarbeitung von Daten, welche Auftraggeber in d.velop Cloud-Produkten speichern, erfolgt nicht in Rechenzentren der d.velop AG, sondern in separaten Rechenzentren. Diese können den jeweiligen Leistungsbeschreibungen der Produkte entnommen werden kann.

3.1 Zutrittskontrolle

3.1.1 d.velop campus

Der d.velop campus in Gescher ist der Hauptstandort der d.velop AG.

3.1.1.1 Zutrittskontrollsystem

Alle d.velop Gebäude auf dem d.velop campus verfügen über ein elektronisches Zutrittskontrollsystem, welches mit Bewegungsmeldern und Alarmanlagen gekoppelt ist. 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 Fernwartungsräumlichkeiten befindet sich im 1. Obergeschoss und verfügt über einen zusätzlichen Sichtschutz im Gebäude. Alle Beschäftigten verfügen über einen personalisierten Ausweis, um Zutritt in die verschlossenen Gebäude zu erhalten.

3.1.1.2 Empfang und Besucherregelung

In Zentralgebäude werden Besucher der d.velop-Unternehmen empfangen. Der Empfang ist während der Geschäftszeiten ständig besetzt. Das Empfangspersonal registriert Besucher und begleitet die Besucher in die Besprechungsräume. Ein selbständiges Bewegen von Besuchern in den anderen Gebäuden ist nur in Ausnahmefällen und ausschließlich in Begleitung von d.velop Mitarbeitenden gestattet.

3.1.1.3 Workflow zur Erteilung von Zutrittsberechtigungen

Die Zutrittsberechtigungen werden über ein workflowbasiertes System vergeben. Die d.velop Mitarbeitenden müssen dazu einen elektronischen Zutrittsberechtigungsantrag stellen.

3.1.1.4 Sicherheitszonen

Innerhalb der Firmengebäude befinden sich einzelne Sicherheitsbereiche. Diese Sicherheitsbereiche sind durch weitere technische Maßnahmen abgesichert. Die Sicherheitszonen sind für Außenstehende nicht erkenntlich und werden nur in einem internen Dokument zur IT-Sicherheit aufgeführt. Die Sicherheitsbereiche umfassen unter anderem die Technikräume, die Räume von Geschäftsführung, HR und IT-Administration.

3.1.2 Weitere Standorte der d.velop AG oder verbundener Töchter

Neben dem Hauptstandort am d.velop campus in Gescher gibt es weitere Standorte, welche mindestens die nachfolgenden Anforderungen erfüllen:

- Elektronisches Zutrittskontrollsystem bzw. zentrales physikalisches Schließsystem
- Verschlossene Gebäude
- Besucherregelung (sofern Kunden-/Partnerverkehr)

3.1.3 Physische Sicherheit für d.velop Cloud-Produkte

d.velop betreibt Cloud-Produkte ausschließlich bei Rechenzentrumsbetreibern mit einer gültigen Zertifizierung nach ISO/IEC 27001. Diese verfügen daher untern anderem über folgende technische und organisatorische Maßnahmen zur physischen Sicherheit:

- Definierte physische Sicherheitszonen
- Elektronische Zutrittskontrollsysteme für ausschließlich autorisiertes Personal
- Besucherregelung
- Geschultes Sicherheitspersonal
- Videoüberwachung

3.2 Zugangskontrolle

3.2.1 Benutzername & Kennwort

Die d.velop AG betreibt für alle d.velop-Unternehmen ein zentralen Verzeichnisdienst, welcher für die Anmeldung an allen produktiven Endgeräten und Servern verwendet wird. Die Vergabe von Benutzerkonten erfolgt für Mitarbeitende ausschließlich personalisiert.

3.2.2 Kennwortrichtlinie

Eine interne Richtlinie zum Access- und Password Management gibt vor, welche Anforderungen an ein Kennwort bestehen. Die Kennwortrichtlinie orientiert sich am aktuellen Stand der Technik und folgt Empfehlungen anerkannter Stellen (u.a. NIST und BSI).

3.2.3 Multi-Faktor Authentifizierung

d.velop verwendet Multi-Faktor Authentifizierung. Die Aufforderung zur Eingabe des zweiten Faktors erfolgt abhängig davon, von welchem Endgerät der Zugriff erfolgt und welchen Schutzbedarf das jeweilige IT-System hat.

3.2.4 Single-Sign-On

Wenn IT-Systeme Single-Sign-On unterstützen, wird dieser Mechanismus verpflichtend aktiviert. Für Systeme ohne einen solchen Mechanismus definiert eine interne Richtlinie zum Access- und Password Management verbindliche Anforderungen.

3.2.5 Autorisierungsprozess für Zugangsberechtigungen

Zugangsberechtigungen zu IT-Systemen werden ausschließlich personalisiert vergeben. Die Anlage neuer Benutzerkonten für d.velop Mitarbeitende erfolgt im Rahmen des Onboarding-Prozesses, welche durch die interne HR-Abteilung initiiert wird. Die Vergabe von (zusätzlichen) Zugangsberechtigungen erfolgt, wo möglich rollenbasiert und immer schriftlich.

3.2.6 Zugang zu d.velop Cloud-Produkten

Der Zugang zu Cloud-Produkten erfolgt mit personalisierten Accounts und unter Verwendung der zuvor beschriebenen Sicherheitsmaßnahmen. Für die automatisierte Bereitstellung von Infrastruktur und Updates werden eingeschränkte Serviceaccounts verwendet.

3.2.7 Autorisierungsprozess für Zugangsberechtigungen zu Cloud-Produkten

Zugangsberechtigungen zu Cloud-Produkten werden ausschließlich nach dem Principle of Least Privilege vergeben. Die Vergabe erfolgt für Mitarbeitende durch einen geregelten und nachvollziehbaren Workflow über das interne Ticketsystem.

3.2.8 Protokollierung von Zugangsversuchen zu Cloud-Produkten

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

3.2.9 Zugang zu Kundensystemen (On Premises-Fernwartung)

Gängige Fernwartungsverfahren sind das aktive Aufschalten mittels einer Fernwartungslösung (z.B. TeamViewer) im Beisein des Auftraggebers, sowie die Verwendung einer Client-VPN-Software mit anschließender Remote

Sitzung (Remote Desktop). d.velop richtet sich dabei nach den Vorgaben des Auftraggebers. Bei allen Verfahren wird der Zugang zu den Systemen des Auftraggebers durch den Auftraggeber selbst kontrolliert.

3.2.10 Firewall Systeme

Zum Schutz vor ein unerwünschtes Eindringen werden Firewall Systeme mit IDS- und IPS-Funktionalität verwendet. IT-Systeme, die aus dem Internet erreichbar sind, sind ausschließlich benötigte Schnittstellen freigegeben.

d.velop Cloud-Produkte 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 so weit von extern freigeschaltet, wie erforderlich (bspw. Port 443 für HTTPS-Freigabe der Frontendserver zur Kommunikation mit dem Kunden).

3.2.11 Endpoint Detection and Response -Lösungen

Zum Schutz vor Schadsoftware wird eine Endpoint Detection and Response (EDR) Lösung verwendet. Die Aktualisierung der Signaturen erfolgt automatisiert. Auf allen internen produktiven Endgeräten (Server, PCs, Notebooks) ist dieser Virenschutz eingerichtet und aktiviert.

d.velop Cloud-Produkte verwenden, wo technisch sinnvoll, EDR-Lösungen. Diese dient primär dem Selbstschutz der d.velop Infrastruktur und ist nicht explizit Bestandteil der Leistungsbeschreibung.

3.2.12 Spamschutzlösung

Zum Schutz vor unerwünschten E-Mails (Phishing und Spam) und auch zum Schutz vor Schadsoftware ist eine Spamschutzlösung installiert. Für alle eingehenden E-Mails wird automatisiert eine Spam-Überprüfung vorgenommen.

3.2.13 Bildschirmschoner mit Kennwortschutz

Bei Inaktivität eines Arbeitsplatzes wird ein Bildschirmschoner mit Kennwortschutz aktiviert. Der Bildschirmschoner mit Kennwortschutz wird spätestens nach 10 Minuten automatisch aktiviert. Die Mitarbeitenden sind organisatorisch über eine Richtlinie angewiesen, unabhängig hiervon den Bildschirm beim Verlassen des Arbeitsplatzes immer sofort zu sperren.

3.3 Zugriffskontrolle

Der Zugriff auf die IT Systeme durch die d.velop-Unternehmen erfolgt ausschließlich bedarfsorientiert und nach dem „Need to know Prinzip“. Alle Mitarbeitenden in den d.velop Unternehmen erhalten nur Zugriff auf die IT Systeme, welche für die Erfüllung der täglichen Arbeit unbedingt notwendig sind.

3.3.1 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.

Die Vergabe von zusätzlichen Zugriffsberechtigungen erfolgt ausschließlich schriftlich.

3.3.2 Klassifizierung von Informationswerten

Eine Richtlinie zur Klassifizierung von Informationen definiert die Mindestanforderungen an die Klassifizierung von digitalen und analogen Informationen hinsichtlich ihrer Vertraulichkeit und legt Regeln zur entsprechenden Kennzeichnung sowie zum richtigen Umgang mit Informationen entsprechend ihrer Klassifizierung fest.

3.3.3 Akten- und Datenträgervernichtung

Für die Entsorgung von Datenträgern und Dokumenten sind in ausgewiesenen Bereichen Datenschutztonnen und Dokumentenvernichter aufgestellt. Die Entsorgung wird im Auftrag der d.velop AG von zertifizierten Unternehmen datenschutzkonform durchgeführt. Die Vernichtung der über die Datenschutztonnen entsorgten Dokumente erfolgt über Maschinen, welche gemäß DIN 66399 arbeiten.

3.4 Trennungskontrolle

d.velop verwendet für Trennung von IT-Systemen sowohl physikalisch als auch logisch getrennte Systeme.

3.4.1 Trennung von Entwicklungs-, Test- und Produktivumgebung

Sämtliche IT-Systeme sind in Entwicklungs-, Test- und Produktivumgebung unterteilt. Der Zugriff zu den einzelnen Umgebungen ist mit bedarfsgerechten Zugriffsberechtigungen versehen. Das Einspielen von neuen Produktversionen erfolgt grundsätzlich in einem mehrstufigen Prozess, bei welchem zuerst Testumgebungen zur Funktionsprüfung verwendet werden. Der Kreis zugriffsberechtigter Mitarbeitender auf Test- und -Produktivumgebungen der d.velop Cloud-Produkte ist auf Personengruppen beschränkt, für welche ein Zugriff zur Aufgabenerfüllung unbedingt notwendig ist.

3.4.2 Mandantentrennung innerhalb von d.velop Cloud-Produkten

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

3.4.3 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 Mitarbeitende.

3.5 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-Produkten abgelegt werden. Im Übrigen obliegt es dem Kunden als Anwender der Cloud-Produkte, die von ihm zur Verarbeitung offengelegten personenbezogenen Daten bei Bedarf zu pseudonymisieren.

3.6 Schulung von Mitarbeitenden

Alle Mitarbeitenden absolvieren jährlich Pflichtschulungen in den Bereichen IT-Sicherheit und Datenschutz. Zusätzliche anlassbezogene Maßnahmen sensibilisieren darüberhinausgehend. Neue Mitarbeitende absolvieren die Schulungen im Rahmen des Einarbeitungsprozesses.

3.7 Homeoffice und mobiles Arbeiten

Homeoffice und mobiles Arbeiten sind ausschließlich gemäß Vorgaben einer für die Mitarbeitenden verbindlichen IT-Richtlinie zulässig. Diese gewährleistet, dass der Arbeitsplatz den Vertraulichkeitsanforderungen der d.velop-Gruppe entspricht, die Verwendung privater Hardware auf ein Minimum (Internetanschluss, Peripheriegeräte, Monitore) zu begrenzen ist, die Entsorgung von Unterlagen und Datenträgern nicht unterwegs oder im Homeoffice erfolgt und dass Endgeräte stets sicher zu verwahren sind. Darüberhinausgehende besondere Anforderungen oder Verbote von Auftraggebern werden beachtet.

3.8 Sichere Softwareentwicklung und -betrieb

Um einen sicheren Software Development Lifecycle (SSDLC) umzusetzen verfolgt d.velop eine Shift-Left-Strategie. Wesentliche Aspekte dazu sind in der internen Richtlinie Informationssicherheit und Datenschutz im Bereich Softwareentwicklung und -betrieb definiert. Die Einhaltung wird regelmäßig überprüft.

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

4.1 Weitergabekontrolle

4.1.1 Transportverschlüsselung

Sämtliche extern erreichbare IT-Systeme und d.velop Cloud-Produkte verwenden Transportverschlüsselung (z.B. HTTPS). Sie sind ausschließlich über verschlüsselte Kommunikationswege erreichbar. Die Verschlüsselung erfolgt gemäß dem Stand der Technik (u.a. BSI TR-02102).

4.1.2 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 FileVault, Apple iOS-Geräteverschlüsselung) realisiert.

4.1.3 Verschlüsselung von Funk-Netzwerken

Sämtliche Funk-Netzwerke (WLAN), welche interne Systeme erreichen, kommunizieren ausschließlich verschlüsselt. Die Netzwerke sind für unterschiedliche Interessengruppen (Mitarbeitende, Schulungsteilnehmer) aufgeteilt. Aus Netzwerken, die Externen zugänglich sind (Schulung, Gast), ist kein Zugriff auf interne IT-Systeme möglich.

4.2 Eingabekontrolle

Audit-Logs gewährleisten eine Nachvollziehbarkeit getätigter Eingaben und Änderungen.

4.2.1 Dokumenten Management System (DMS)

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

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

5.1 Notfallpläne

Zentrale Notfallpläne und konkrete Handlungsanweisungen werden fortlaufend aktualisiert und berücksichtigen aktuelle Risiken (u.a. Ransomware, Elementarschäden, Ausfall einzelner IT-Systeme). Regelmäßige Übungen gewährleisten, dass die Pläne allen beteiligten Personen vertraut sind und der Umgang mit selbigen funktioniert.

5.2 Sicherungskonzept

Produktive Daten und IT-Systeme werden regelmäßig gesichert. Die Häufigkeit und Dauer der Aufbewahrung beziehen sich dabei auf die Sensibilität der gesicherten Daten. Sicherungsintervalle für d.velop Cloud-Produkte können den jeweiligen Leistungsbeschreibungen entnommen werden.

5.3 Einspielen von Sicherheitsupdates

Sämtliche produktive IT-Systeme werden regelmäßig aktualisiert. Sicherheitsupdates für produktive Endgeräte werden zeitnah nach dem Erscheinen eingespielt. Vorgelagerte Tests gewährleisten, dass die Updates problemlos eingespielt werden können.

Zentrale IT-Systeme und d.velop Cloud-Produkte werden regelmäßig in geplanten Wartungsfenstern aktualisiert. Im Falle von außerplanmäßig bekanntgewordenen kritischen Sicherheitslücken erfolgt ein umgehendes Einspielen entsprechender Patches.

5.4 Deployment Prozess

Die d.velop-Gruppe hat einen Deployment Prozess etabliert, welcher für alle d.velop Cloud-Produkte implementiert ist. Sämtliche Änderungen an Cloud-Produkten werden dokumentiert und versioniert. Die Entwicklung und das Einspielen neuer Funktionalitäten erfolgen 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.

5.5 Schwachstellen- und Belastbarkeitstests

Es werden regelmäßig intern und extern beauftragte Schwachstellen- und Belastbarkeitstests durchgeführt. Diese gewährleisten, dass Schwachstellen oder andere Defizite rechtzeitig festgestellt und behoben werden.

5.6 Überwachung der IT-Systeme

d.velop verwendet für die Überwachung der IT-Systeme verschiedene Monitoring- und Alarmierungssysteme. Definierte Alarme informieren unverzüglich über Abweichungen vom Normalbetrieb. Dies ermöglicht eine sofortige Erkennung von Fehlverhalten und eine verkürzte Zeit zur Wiederherstellung des Normalbetriebs.

5.7 Redundanzen

Kritische IT-Systeme und Versorgungseinrichtungen (u.a. Stromzufuhr, USV) sind redundant ausgelegt, sodass ein ausfallfreier Betrieb gewährleistet werden kann. Die IT-Systeme sind dabei so verteilt, dass einzelne Brandabschnitte/Verfügbarkeitszonen ausfallen können.

5.8 Technische Überwachung der Rechenzentren

Die von d.velop beauftragten Rechenzentren verwenden Messtechniken zur frühzeitigen Erkennung von möglicherweise eintretenden Elementarschäden (Feuer, Wasser). Systeme wie Unterbrechungsfreie Stromversorgungen (USV) und Löschanlagen gewährleisten, dass bei etwaigen auftretenden Schäden eine weitreichende Zerstörung vermieden werden kann.

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

6.1 Datenschutz-Management

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

6.1.1 Datenschutzleitbild

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

6.1.2 Datenschutz-Richtlinie

Die d.velop AG hat durch den Vorstand eine gruppenweite 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-Gruppe getroffenen und u.a. in diesem Dokument dokumentierten Maßnahmen und implementierten Geschäftsprozessen zum Datenschutz.

6.1.3 Benennung eines Datenschutzbeauftragten

Die d.velop-Unternehmen haben, soweit gesetzlich verpflichtend, einen externen Datenschutzbeauftragten benannt. Der externe Datenschutzbeauftragte der d.velop AG ist seit dem 01.10.2021 Herr Nils Möllers. Der externe Datenschutzbeauftragte der d.velop AG hat die erforderliche Fachkunde zum Ausüben der Tätigkeit des betrieblichen Datenschutzbeauftragten. Er ist zertifizierter Datenschutzbeauftragter und verfügt über mehrjährige Erfahrung auf dem Feld der Datenschutzberatung.

Die Kontaktdaten des Datenschutzbeauftragten lauten:

Nils Möllers
Keyed GmbH
Siemensstraße 12, 48341 Altenberge
datenschutz@d-velop.de

Der externe Datenschutzbeauftragte der d.velop AG ist direkt dem Vorstand der d.velop AG unterstellt und berichtet somit gemäß Art. 38 Abs. 3 S. 3 DSGVO unmittelbar der höchsten Managementebene des Verantwortlichen. Die d.velop AG stellt zudem sicher, dass der externe Datenschutzbeauftragte in Ausübung seiner Tätigkeit auf dem Gebiet des Datenschutzes gemäß Art. 38 Abs. 3 S. 1, 2 DSGVO weisungsfrei ist.

6.1.4 Berichtswesen

Der externe Datenschutzbeauftragte hat die Möglichkeit, direkt an den Vorstand der d.velop AG zu berichten. Es finden zweiwöchentlich Status-Meetings statt, an denen auch der Informationssicherheitsbeauftragte sowie bei Bedarf der Vorstand und die Rechtsabteilung teilnehmen.

Neben den Statusmeetings werden Berichte und Anfragen direkt per E-Mail kommuniziert. Weiterhin werden wesentliche Entscheidungen in einem Tätigkeitsbericht des externen Datenschutzbeauftragten festgehalten.

6.1.5 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 Vorstand (Berichtswesen). Die Tätigkeitsberichte sind vertraulich und nur für den externen Datenschutzbeauftragten und den Vorstand bestimmt.

6.1.6 Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

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

6.1.7 Qualitätsmanagementsystem

Die d.velop betreibt ein Qualitätsmanagementsystem, welches eine Vielzahl von Arbeitsanweisungen, Verfahrensanweisungen, Richtlinien und Merkblätter beinhaltet. Diese sind für das Datenschutzmanagement in allen d.velop-Unternehmen verbindlich.

6.1.8 IT-Sicherheits- und Datenschutzteam

Die d.velop AG hat ein IT-Sicherheits-, Geheimnisschutz- und Datenschutzteam (siehe oben). Es trifft sich regelmäßig alle zwei Wochen.

6.1.9 Verpflichtung der Mitarbeitenden

Alle Mitarbeitenden der d.velop-Unternehmen werden dokumentiert auf die Vertraulichkeit (früher: das Datengeheimnis gemäß § 5 BDSG), das Sozialgeheimnis (§ 35 SGB I), auf die Wahrung von Geschäftsgeheimnissen (GeschGehG) und Berufsgeheimnissen (§ 203 StGB) sowie bei Bedarf auf das Fernmeldegeheimnis (§ 3 TTDSG) und das Bankgeheimnis verpflichtet. Diese Verpflichtungserklärung ist fester Bestandteil des Arbeitsvertrages und Teil der Personalakte. Der Verpflichtungserklärung ist ein Merkblatt beigefügt, in welchem die Bedeutung dieser einzelnen Paragraphen erläutert wird.

6.1.10 Schulungsmaßnahmen

Die Datenschutzunterweisung ist Bestandteil des Einstellungsverfahrens für neue Mitarbeitende. Im Rahmen dieses Einstellungsverfahrens findet sowohl eine Unterweisung bezüglich des Datenschutzes gemäß DSGVO statt als auch eine Unterweisung bezüglich des Sozialgeheimnisses (SGB). Neben diesen Schulungen werden aktuelle Themen rund um den Datenschutz über das Intranet der d.velop-Gruppe an die Mitarbeitenden herangetragen. Die E-Mail-Adresse datenschutz@d-velop.de steht zudem allen Mitarbeitenden zur Verfügung, um Fragen und Datenschutzvorfälle an den externen Datenschutzbeauftragen zu richten.

6.1.11 Intranet und Datenschutzportal

Aktuelle Neuigkeiten und Änderungen bezogen auf den Datenschutz, die IT Sicherheit und den Geheimnisschutz der d.velop-Gruppe werden sowohl in Mitarbeiterversammlungen als auch im Intranet der d.velop-Gruppe veröffentlicht. Über das Intranet haben Mitarbeitende Zugriff auf alle relevanten Dokumente zum Datenschutz.

6.2 Management bei Datenschutzverletzungen

Beim Verdacht auf eine Datenschutzverletzung gibt es einen in der d.velop-Gruppe festgelegten und beschriebenen Informationslauf, der gewährleistet, dass durch das Statusteam (siehe oben) unverzüglich der Sachverhalt geprüft werden kann. Die Eingangsmeldungen erfolgen hierbei stets über incidents@d-velop.de, damit Datenschutzbeauftragter, Informationssicherheitsbeauftragter, Leitung IT und Rechtsabteilung sofort

informiert sind. Soweit erforderlich werden von dort 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.

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

Die von der d.velop-Gruppe 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-Gruppe sind als solche gekennzeichnet, eine Verpflichtung zum Ausfüllen besteht selbstverständlich nicht.

6.4 Auftragskontrolle

Die d.velop AG und andere d.velop-Unternehmen als Auftragnehmer unterliegen bei der Auftragsverarbeitung dem Art. 28 DSGVO und ggf. dem § 80 SGB X. Hierbei ist der Auftraggeber als Verantwortlicher für die Einhaltung der datenschutzrechtlichen Vorschriften und Gesetze verantwortlich. Diese Verantwortung des Auftraggebers unterstützen die d.velop-Unternehmen aktiv durch eine Vielzahl von technischen und organisatorischen Maßnahmen. Das Ihnen vorliegende Dokument ist Bestandteil dieser Maßnahmen. Soweit erforderlich schließen die d.velop-Unternehmen mit Ihnen als Kunde einen den gesetzlichen Anforderungen entsprechen-den Vertrag zur Auftragsverarbeitung ab.

6.4.1 Unterauftragnehmer

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

Die d.velop-Unternehmen 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 Auftragsverarbeitung wird dem jeweiligen Hauptauftraggeber in der d.velop-Gruppe immer ein Kontrollrecht, Besichtigungsrecht und Weisungsrecht eingeräumt.

In dem mit einem Kunden abgeschlossenen Vertrag zur Auftragsverarbeitung führt das jeweils als Auftragsverarbeiter tätige d.velop-Unternehmen die als Unterauftragnehmer (weitere Auftragsverarbeiter) eingesetzten Tochtergesellschaften sowie ggf. zusätzlich als Unterauftragnehmer eingesetzte, 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-Unternehmen werden regelmäßig durch Kunden oder externe Dritte (z.B. Prüfgesellschaften) auditiert. Etwaige bei den Audits ausgesprochene Empfehlungen werden im Nachgang vom IT-Sicherheits-, Geheimnisschutz- und Datenschutzteam (siehe oben) bewertet und hiernach umgesetzt, wo erforderlich oder zur Verbesserung des Datenschutzes sinnvoll.

Sämtliche Leistungsbeziehungen der d.velop-Unternehmen zu ihren Kunden und Unterauftragnehmern werden im DMS (siehe oben) dokumentiert und transparent gemacht. So ist jederzeit feststellbar, für wen die d.velop-Unternehmen mit welchen Unterauftragnehmern welche Leistungen erbringt.

7 Besondere Geheimhaltungsmaßnahmen

§ 2 Nr. 1 Buchst. b) Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) verlangt, dass der rechtmäßige Inhaber den Umständen nach angemessene Geheimhaltungsmaßnahmen zu Schutz von Geschäftsgeheimnissen festzulegen hat. Die nachfolgend beschriebenen Maßnahmen gelten ergänzend zu den vorbenannten Maßnahmen für alle von der d.velop-Gruppe erlangten und genutzten Geschäftsgeheimnisse und andere vertrauliche Informationen.

7.1 Festlegung verbindlicher Verhaltensregeln

Alle d.velop-Unternehmen haben sich verbindlichen Verhaltensregeln zum Geheimnisschutz, Datenschutz und zur Informationssicherheit unterworfen. Dieses Schutzkonzept ist Teil dieser Verhaltensregeln, die vollständig im Serviceportal der d.velop AG veröffentlicht sind. Mit den Verhaltensregeln wird sichergestellt, dass innerhalb der d.velop-Gruppe in jedem Unternehmen ein gleichermaßen hohes Schutzniveau gewährleistet ist.

7.2 Abschluss von Geheimhaltungsvereinbarungen

Die d.velop-Unternehmen haben untereinander Geheimhaltungsvereinbarungen abgeschlossen (Non Disclosure Agreements, NDA). Diese sind ein weiterer Bestandteil der Verhaltensregeln (siehe oben). Außerdem schließt die d.velop-Unternehmen mit ihren Kunden marktübliche, den gesetzlichen Anforderungen des Gesetzes zum Schutz von Geschäftsgeheimnissen entsprechende Geheimhaltungsvereinbarungen und reichen diese in der Leistungskette an etwaige Unterauftragnehmer und Dritte durch.