OPTIMAL SYSTEMS

Datenschutzkonzept

Unternehmenserklärung zum Datenschutz und Datensicherheit

Version 2.1

Gültig ab: 06.09.2018

OPTIMAL SYSTEMS GmbH
Unternehmenszentrale
Cicerostraße 26
10709 Berlin

Änderungsübersicht

Datum	Name	Änderung	Version
01.04.2011	Björn Grabe	Erstellung	1.0
06.05.2013	Alexander Tonn	Review und Ergänzung Kapitel 5.2.8	1.1
27.05.2015	Alexander Tonn	Review und Anpassung Produktbezeichnung	1.2
05.01.2018	Norbert Vogel	Überarbeitung EU-DSGVO	2.0
04.09.2018	Norbert Vogel	Überarbeitung BDSG	2.1

Freigabeinformationen

Version	Erstellt durch	Erstelldatum	Unterschrift	Freigabe durch	Freigabedatum	Unterschrift
1.0	Björn Grabe	02.05.2011	<digital>	Mirko Putz	02.05.2011	<digital>
1.1	Alexander Tonn	07.05.2013	<digital>	Alexander Tonn	07.05.2013	<digital>
1.2.	Alexander Tonn	27.05.2015	<digital>	Alexander Tonn	27.05.2015	<digital>
2.0	Norbert Vogel	05.01.2018	<digital>	Björn Grabe	05.01.2018	<digital>
2.1	Norbert Vogel	04.09.2018	<digital>	Gregor Wolf	06.09.2018	<digital>

Inhaltsverzeichnis

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

1 Einleitung

1.1 Zweck und Geltungsbereich

Mit diesem Dokument wird das grundsätzliche Verständnis von Datenschutz und Datensicherheit insbesondere im Umgang mit auftragsbezogenen Kundendaten, aber auch darüber hinaus, für die OPTIMAL SYSTEMS GmbH (OS) postuliert und sich daraus ableitende Handlungsrichtlinien definiert.

Als Softwarehersteller und Lösungsanbieter im Bereich Enterprise Content Management ergeben sich im täglichen Betrieb des Unternehmens vielfältige Berührungspunkte mit datenschutzrelevanten Bereichen. So kommt es im Zusammenhang mit der Einführung unseres Produktes enaio® bei Kunden immer dazu, dass im Rahmen der Tätigkeit auf Kundendaten zugegriffen wird oder diese zu Analysezwecken OPTIMAL SYSTEMS zur Verfügung gestellt werden. Gleiches gilt für den Bereich der technischen Kundenbetreuung und des Supports.

Nach Artikel 28ff – Auftragsverarbeiter - der EU-Datenschutzgrundverordnung (DS-GVO) und § 63 Bundesdatenschutzgesetz (BDSG) – Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag – ist bei der Auftragsdatenverarbeitung jeweils der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer bereichsspezifischer Regelungen zum Datenschutz verantwortlich. Aus diesem Grunde werden üblicherweise individuelle Datenschutzvereinbarungen zwischen OPTIMAL SYSTEMS und dem jeweiligen Auftraggeber vereinbart.

1.2 Gültigkeitsbereich

Dieses Dokument gilt für alle Bereiche und Mitarbeiter der OPTIMAL SYSTEMS GmbH und deren hundertprozentiger Tochterunternehmen und hat für alle Angestellten des Unternehmens verbindlichen Charakter.

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

1.3 Zuständigkeiten

1.3.1 OPTIMAL SYSTEMS

Die Review und Genehmigung dieses Dokumentes erfolgt durch den Geschäftsbereichsleiter Professional Services und den Datenschutzbeauftragten des Unternehmens.

Dieses Dokument unterliegt einem Review innerhalb von maximal 3 Jahren. Dafür ist der Datenschutzbeauftragte des Unternehmens verantwortlich.

1.3.2 Qualitätsoperationen

Review dieses Dokumentes durch einen Qualitätsmanager

2 Begriffe und Definitionen

Die im vorliegenden Dokument verwendeten Begriffe orientieren sich in ihrer Verwendung an den Definitionen der DIN EN 9001:2000, Kapitel 2 und der im Artikel 4 der DS-GVO festgehaltenen Begriffsbestimmung.

3 Unternehmensstrategie zu Datenschutz und Datensicherheit

Die Unternehmensstrategie wurde durch die Geschäftsführung der OPTIMAL SYSTEMS GmbH wie folgt definiert:

1. Das Tätigkeitsfeld der OPTIMAL SYSTEMS GmbH bedingt hohe Anforderungen an Datenschutz und Datensicherheit. Im Rahmen der Kundenbeziehungen erhält die OPTIMAL SYSTEMS tiefe Einblicke in die Unternehmensprozesse und die damit verbundenen Daten ihrer Kunden. Darüber hinaus kommt es zum Zugriff auf schützenswerte Daten Dritter, z.B. Patientendaten in einem Krankenhaus.

   Aus diesem Grunde stellt der Datenschutz und die Datensicherheit eines der wichtigsten Qualitätsziele des Unternehmens dar und ist in das zertifizierte Qualitätsmanagementsystem integriert.

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

2. Datenschutz und Datensicherheit umfassen bei OPTIMAL SYSTEMS
   - den Schutz personenbezogener Daten gemäß den gesetzlichen Vorschriften des BDSG und anderer Vorschriften über den Datenschutz,
   - die Sicherheit bei der Verarbeitung vertraulicher Personen- und Betriebsdaten des Kunden,
   - die Gewährleistung des störungsfreien Betriebs der Informationstechnik (IT-Sicherheit) als Voraussetzung für eine sichere Verarbeitung.
3. Datenschutz und Datensicherheit sind in das Management des Unternehmens integriert. Die Führungskräfte der Unternehmensbereiche tragen die persönliche Verantwortung für die Durchsetzung der dazu getroffenen Festlegungen.
4. Die konkreten Maßnahmen und die Verantwortlichkeiten sind detailliert in firmeninternen Verfahrens- und Arbeitsanweisungen festgelegt und werden im Rahmen des Qualitätsmanagementsystems der Firma sowohl extern als auch intern auditiert und bewertet.
5. Der Beauftragte für den Datenschutz wirkt auf die Einhaltung des Bundesdatenschutzgesetzes, der DS-GVO sowie anderer Vorschriften über den Datenschutz hin. Durch die Einflussnahme auf die Gestaltung der innerbetrieblichen Organisation im Sinne des Artikel 25 ff. DS-GVO, sowie § 64 BDSG (technische und organisatorische Maßnahmen) unterstützt er den IT-Sicherheitsprozess und die Datensicherheit insgesamt.
6. Die Mitarbeiter des Unternehmens werden durch die persönliche, vertragliche Verpflichtung auf das Datengeheimnis sowie durch angemessene Schulungen und periodische Unterweisungen motiviert und befähigt, die vorgegebenen Festlegungen zu Datenschutz und Datensicherheit an ihrem Arbeitsplatz zuverlässig und ordnungsgemäß einzuhalten.

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

4 Organisation von Datenschutz und Datensicherheit

4.1 Definition von Schutzstufen

Ausgehend von der Datenschutzstrategie und dem individuellen Schutzbedarf von Kundendaten sind für die Unternehmensbereiche der OPTIMAL SYSTEMS folgende Schutzstufen festgelegt:

- ein Grundschutz, der für alle Unternehmensbereiche und Geschäftsstellen der Firma verbindlich ist,
- und ein erweiterter Datenschutz, der je nach den individuellen Erfordernissen der einzelnen Unternehmensbereiche und der jeweiligen Kundenbeziehung einzuhalten ist.

4.2 Grundschutz

Der durch OPTIMAL SYSTEMS gewährleistete allgemein verbindliche Grunddatenschutz umfasst folgende Maßnahmen:

- die Durchsetzung der auf der Grundlage der DS-GVO und des BDSG festgelegten Maßnahmen des Schutzes personenbezogener Daten,
- die technischen und organisatorischen Maßnahmen der Datensicherung gem. Artikel 28ff DS-GVO sowie § 64 BDSG, die auch bei der Auftragsverarbeitung vertraulicher Personen- und Betriebsdaten anzuwenden sind,
- die für die konkreten Betriebsbedingungen zutreffenden Verfahren der IT-Sicherheit.

4.3 Erweiterter Datenschutz

Die erweiterten Datenschutzmaßnahmen werden durch die jeweils zuständigen Geschäftsbereichsleiter in enger Zusammenarbeit mit den Kunden und dem Datenschutzbeauftragten festgelegt.

Dabei wird u. a. folgendes berücksichtigt:

- Gegenstand und Ziele der speziellen Festlegungen,
- einzuleitende zusätzliche Schutzmaßnahmen, die über die Festlegungen für den Grunddatenschutz hinausgehen,
- der zusätzliche finanzielle, personelle und technische Aufwand und dessen Realisierung,
- Zuständigkeiten und Verantwortung für die Einführung und Kontrolle.

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

Die mit den Kunden individuell vereinbarten Datenschutzvereinbarungen werden den davon betroffenen Mitarbeitern des Unternehmens nachweislich zur Kenntnis gebracht.

4.4 Kontrolle und Bewertung

Durch die in allen Unternehmensbereichen vom Datenschutzbeauftragten und dem Qualitätsmanager durchgeführten internen Audits und deren Bewertung durch die Geschäftsführung wird eine permanente Weiterentwicklung des Datenschutzsystems gewährleistet.

5 Maßnahmen zu Datenschutz und Datensicherheit

5.1 Maßnahmen des Datenschutzes nach DS-GVO und BDSG

5.1.1 Beauftragter für den Datenschutz

Die OPTIMAL SYSTEMS GmbH hat gemäß Artikel 37 DS-GVO bzw. § 38 BDSG einen Beauftragten für den Datenschutz bestellt. Dieser ist der Geschäftsführung berichtspflichtig, führt in dessen Auftrag periodisch und zu speziellen Sicherheitsmaßnahmen Kontrollen und Audits durch und unterbreitet Vorschläge zur kontinuierlichen Vervollkommnung von Datenschutz und Datensicherheit im Unternehmen.

Schwerpunkt seiner Tätigkeit ist neben der Gewährleistung des Schutzes personengebundener Daten der Mitarbeiter die Sicherheit der nach Artikel 28 DS-GVO und § 63 BDSG im Auftrag zu verarbeitenden Kundendaten.

Dabei arbeitet er eng mit den für die Verarbeitung der Daten verantwortlichen Geschäftsbereichsleitern zusammen und nimmt Einfluss auf die Einbeziehung der Datenschutzmaßnahmen in die Arbeitsprozesse des Unternehmens.

5.1.2 Verpflichtungen

Alle Mitarbeiter der OPTIMAL SYSTEMS GmbH werden in ihrem Arbeitsvertrag neben ihrer Verschwiegenheitspflicht unterschriftlich auf das Datengeheimnis nach Artikel 29 DS-GVO und § 53 BDSG verpflichtet und darüber belehrt, dass Verstöße dagegen ggf. nach Artikel 9 und 10 der

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

DS-GVO und §§ 41/42 BDSG und anderen einschlägigen Rechtsvorschriften geahndet werden und mit arbeitsrechtlichen Maßnahmen verbunden sein können.

Darüber hinaus erfolgt üblicherweise auf Wunsch von Kunden aus bestimmten Branchen bei der Verarbeitung besonders sensibler Kundendaten oder bei besonderen Verarbeitungsbedingungen, z.B. ein Direktzugriff auf produktive IT-Systeme der Kunden, eine spezielle Verpflichtung der betreffenden Mitarbeiter nach einem vorgegebenen Verpflichtungstext des Kunden.

5.1.3 Unterweisungen

OPTIMAL SYSTEMS führt periodisch (in der Regel jährlich) oder zu besonderen Anlässen Datenschutzschulungen durch mit dem Ziel, ihre Führungskräfte und alle Mitarbeiter für die Durchsetzung des Datenschutzes zu sensibilisieren und zu motivieren, ihr Verständnis und ihre Unterstützung für die festgelegten Maßnahmen zu erreichen sowie sie zu befähigen, die festgelegten Sicherheitsmaßnahmen korrekt und sinnvoll anzuwenden.

Darüber hinaus besteht auf Kundenwunsch die Möglichkeit, zu bestimmten Anwendungen der Auftragsverarbeitung neben der allgemeinen Einweisung spezielle Unterweisungen zu Fragen des Datenschutzes durchzuführen.

5.1.4 Kontrollen und Audits

Durch die vom Datenschutzbeauftragten und dem Qualitätsmanager jährlich durchgeführten internen Audits und deren Bewertung durch die Geschäftsführung wird eine permanente Weiterentwicklung des Datenschutzsystems gewährleistet. Davon unberührt bleibt die Verpflichtung alle Führungsebenen des Unternehmens mindestens quartalsweise die Einhaltung der Datenschutzbestimmung für ihren Zuständigkeitsbereich zu kontrollieren.

Auf Wunsch von Kunden besteht nach vorheriger Abstimmung die Möglichkeit, die Ordnungsmäßigkeit der Auftragsverarbeitung ihrer Daten in den Betriebstätten des Unternehmens persönlich zu kontrollieren.

5.2 Technische und organisatorische Maßnahmen nach Artikel 32 DS-GVO und § 64 BDSG

Die innerbetriebliche Organisation der OPTIMAL SYSTEMS GmbH ist derart gestaltet, dass sie den besonderen Bedingungen des Datenschutzes gerecht wird.

Dazu sind Maßnahmen getroffen, die nachstehenden Anforderungen der Artikel 32 der DS-GVO und der Anlage zu § 64 BDSG zu realisieren. Die getroffenen Festlegungen werden auch auf alle anderen Daten angewendet.

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

Die genaue technische Umsetzung der im Folgenden benannten Maßnahmen ist in der Anlage „Technische und organisatorische Maßnahmen (TOM) zum Datenschutzkonzept“ in der aktuellen Version beschrieben.

Elektronisch vorliegende Kundendaten sind verpflichtend im firmeneigenen ECM-System abzulegen und unterliegen somit automatisch den erweiterten Sicherheits- und Schutzmechanismen von enaio®.

5.2.1 Zutrittskontrolle

Unbefugten wird der Zutritt zu den Betriebsstätten und den Datenverarbeitungsanlagen, mit denen personenbezogene und Kundendaten verarbeitet oder genutzt werden, verwehrt durch

- Sicherung der Räume, in denen Daten gelagert oder verarbeitet werden, durch ein elektronischen Zugangskontrollsystem mit Türöffnern und Sicherheitsschlössern sowie eine nachweisbare RFID-Karten- und Schlüsselausgabe,
- Sichtblenden für von außen einsehbare Verarbeitungs- und Lagerräume,
- Zutrittsordnung für die Betriebsräume und nachweisbare Kontrolle des Aufenthalts betriebsfremder Personen.

5.2.2 Zugangskontrolle

Es wird verhindert, dass Datenverarbeitungssysteme des Unternehmens von Unbefugten genutzt werden können. Dazu werden, wenn keine weitergehenden Forderungen seitens des Auftraggebers vorliegen, nachstehende Maßnahmen realisiert:

- Festlegung der befugten Personen für das Betreten der Datenverarbeitungs- und -Lagerräume,
- Nachweisbare Kontrolle des Aufenthalts betriebsfremder Personen,
- Verpflichtender Passwortschutz.

5.2.3 Zugriffskontrolle

Es wird gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Dies wird erreicht durch

- die Festlegung der Berechtigten und ihrer Befugnisse,
- die Haltung von elektronisch vorliegenden Personen- und Betriebsdaten im firmeneignen ECM-System

- die Begrenzung der Zugriffsmöglichkeiten im ECM-System nur auf bestimmte Datenbestände durch Einschränkung der Sichtbarkeitsrechte,
- das Protokollieren sämtlicher Datenzugriff und –manipulationen durch das ECM-System sowie
- die automatische Erstellung von Versionen von Daten (soweit das für die Datensicherung erforderlich ist).

5.2.4 Weitergabekontrolle

Es wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Zur Gewährleistung der Sicherheit bei der elektronischen Übertragung von Daten werden folgende Maßnahmen wirksam:

- die Einhaltung der durch das Netzwerk festgelegten Protokolle bei der Übertragung über ein lokales Datennetz innerhalb des Unternehmens (in einer kontrollierten Zone),
- die Nutzung von VPN- bzw. HTTPS-Verbindungen zwischen den angeschlossenen Niederlassungen des Unternehmens,
- die Verschlüsselung der zu den Kunden zu übertragenden Dateien mit leistungsfähiger Verschlüsselungs-Software (auf Anforderung des Kunden).

5.2.5 Eingabekontrolle

Es wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in enaio® eingegeben, verändert oder entfernt worden sind.

Dazu werden nachstehende Maßnahmen realisiert:

- die Dokumentation der Eingabeverfahren mit der Möglichkeit der nachträglichen Überprüfung der erfolgten Dateneingaben,
- der Nachweis der organisatorisch festgelegten Zuständigkeiten für die jeweilige Eingabe,
- die Führung einer systemeigenen Protokollierung in enaio® über Datum, Name der Eingebenden und eingegebene Daten.

5.2.6 Auftragskontrolle

Es wird gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

In Realisierung dieser Forderung werden folgende Maßnahmen durchgeführt:

- die eindeutige schriftliche Vertragsgestaltung mit klaren Abgrenzungen der Kompetenzen und Pflichten von Auftraggeber und Auftragnehmer,
- der Nachweis der Übernahme und Übergabe der Daten vom und an den Auftraggeber,
- die detaillierte und eindeutige Einweisung der mit der Verarbeitung beauftragten Mitarbeiter,
- die Kontrolle der korrekten Ausführung der Auftragsverarbeitung unter strikter Beachtung der Maßnahmen zur Datensicherung des eigenen Unternehmens sowie der evtl. zusätzlich gestellten Forderungen des Auftraggebers,
- der sorgsame Umgang mit den maschinenlesbaren Datenträgern und Verhinderung einer Vermischung von Daten und Datenträgern unterschiedlicher Aufträge.

5.2.7 Verfügbarkeitskontrolle

Es wird gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Dafür sind folgende Maßnahmen vorgesehen:

- die allgemeinen Maßnahmen zum Schutz vor zufälliger Zerstörung oder Verlust durch Wasserschäden, Blitzschlag oder Stromausfall,
- die Aufstellung von Feuerlöschgeräten in allen Räumen, in denen Daten verarbeitet oder gelagert werden,
- die Stabilisierung der Verarbeitungssysteme mit Geräten der unterbrechungsfreien Spannungsversorgung (USV),
- die Erstellung von Sicherheitskopien und Protokollieren von Dateiänderungen

5.2.8 Trennungsgebot

Es wird gewährleistet, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt verarbeitet werden.

Dies wird erreicht durch:

- die Begrenzung der Zugriffsmöglichkeiten im firmeneigenen ECM-System nur auf bestimmte Datenbestände durch Einschränkung der Sichtbarkeitsrechte,
- die Trennung von Entwicklungs-, Test- und Produktivsystemen.

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

5.3 Maßnahmen zur Sicherheit der Informationstechnik

Die Gewährleistung einer weitreichenden IT-Sicherheit ist Grundlage für eine Durchsetzung der Ziele zum Datenschutz und zur Datensicherheit.

Für eine ausreichende und angemessene IT-Sicherheit sind in der Firma nachfolgende Maßnahmen wirksam.

5.3.1 IT-Grundschutz

Bei der Organisation der IT-Sicherheit orientiert OPTIMAL SYSTEMS am vom Bundesamt für Sicherheit in der Informationstechnik (BSI) heraus-gegebenen IT-Grundschutz-Katalog.

Die vom BSI gegebenen Empfehlungen für die technischen, organisatorischen, personellen und baulich-infrastrukturellen Standardsicherheitsmaßnahmen zum IT-Grundschutz werden im Unternehmen beachtet, was entscheidend zur Gewährleistung der Verfügbarkeit der IT-Systeme sowie der Wahrung von Vertraulichkeit, Integrität (Korrektheit) und Authentizität (digitale Identität) der Daten beiträgt.

5.3.2 Einsatz des unternehmenseignen ECM-Systems

OPTIMAL SYSTEMS setzt sein eigenes Produkt enaio® als zentrales Werkzeug für die Datenverarbeitung und Datenspeicherung ein. Der Zugriff auf dieses System ist sowohl für die unternehmenszentrale, als auch für die angeschlossenen Tochterunternehmen realisiert. Innerhalb des ECM-Systems wird über ein mehrstufiges Berechtigungssystem und die Durchsetzung einer Mandantentrennung gewährleistet, das nur berechtigte Mitarbeiter auf die für ihre jeweilige Tätigkeit notwendigen Daten zugreifen können.

6 Sicherheitsgarantie für die Kundendaten

Aus der Unternehmenserklärung ist ersichtlich, dass die OPTIMAL SYSTEMS GmbH entsprechend ihrer Unternehmensstrategie über ein umfangreiches und wirkungsvolles System von Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit verfügt.

Geschäftsführung und Mitarbeiter garantieren ein hohes Maß an Sicherheit für die von ihren Kunden zur Auftragsverarbeitung übergebenen Dokumente und Daten.

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de