DSV*Gruppe*

Sicherheitskonzept
EMMA

S2 – für den internen Gebrauch

Version:	**1.1**
Autor:	Paul Pruß
Letzte Änderung:	15.03.2023
Gültig seit:	15.02.2023

Freigabe durch:	Sascha Weider	**Gültigkeit:**	Gültig bis auf Weiteres
Geprüft und abgestimmt mit:	ISDS		

Version	Datum	Autor	Art und Umfang der Bearbeitung	Bemerkungen
1.0	15.02.2023	Paul Preuß	Initiale Erstellung	Keine
1.1	15.03.2023	Paul Preuß	Anpassungen nach ISDS Prüfung	Keine

Inhaltsverzeichnis

A. Allgemeines

A.1 Zweck und Grundsätze

Dieses Sicherheitskonzept wurde gemäß den Anforderungen der ISDS-Konzernregeln erstellt. Etwaige Abweichungen vom Regelwerk sind in diesem Dokument ebenfalls festgehalten.

Der unberechtigten Verarbeitung von Informationen und der Zugriff auf diese wird durch die strukturierte Darlegung des Sicherheitskonzepts vorgebeugt.

Dieses Konzept wurde erstellt, weil in der Applikation personenbezogene Daten nach DSGVO Art. 4 Nr. 1 der Sensitivitätsstufe S2 und höher verarbeitet werden.

A.2 Aktualisierungszyklus

Sofern keine anlassbezogenen Änderungen erfolgen, wird dieses Dokument jährlich im ersten Quartal auf Aktualisierungsbedarf geprüft.

A.3 Mitgeltende Dokumente

Nr.	Titel	Version
1	Architekturbeschreibung und Verschlüsselung Dateiname: D6.1.4_Architekturbeschreibung_Verschluesselung_EMMA Ablageort: https://emma.s-communication.de/emma/datenschutz-zertifikate-technische-massnahmen/	D6.1.4
2	Protokollierungs- und Löschkonzept Dateiname: D6.1.1_Protokollierung_EMMA Ablageort: https://emma.s-communication.de/emma/datenschutz-zertifikate-technische-massnahmen/	D6.1.1
3	ISO 27001 Zertifikat Rechenzentrum Dateiname: ISO 27001 Zertifikat Rechenzentrum Ablageort: https://emma.s-communication.de/emma/datenschutz-zertifikate-technische-massnahmen/	1.0
4	ISO/IEC 27001:2013 Zertifikat Managementsystem Dateiname: ISO/IEC 27001:2013 Zertifikat Managementsystem Ablageort: https://emma.s-communication.de/emma/datenschutz-zertifikate-technische-massnahmen/	1.0

B. Allgemeines

B.1 Produkt-Beschreibung

EMMA ist ein sicherer und komfortabler E-Mail Marketing Manager. Anwender können über das Internet E-Mails versenden und die Performance dieser auswerten.

Es gibt EMMA nur in der Ausführungsvariante Browserversion für alle gängigen Browser.
EMMA wird zusammen mit dem Dienstleister Mailingwork GmbH betrieben.
Weiterführende Informationen zu den einzelnen Funktionen der Anwendung sind auf https://emma.s-communication.de/ zu finden.

B.2 Benutzerkreis und Mandanten

Die Applikation wird von Sparkasseninstituten genutzt. Für jedes Institut ist ein eigener Mandant eingerichtet. Die Administration erfolgt durch den Instituts-Admin der Sparkasse (Benutzeradministration), das EMMA Produkt-Team (Benutzeradministration der Instituts-Admins) und den beauftragten Dienstleister Mailingwork GmbH (IT-Betrieb und IT-Wartung der Mandanten).

B.3 Zugriff

Die Oberfläche ist passwortgeschützt und nur über eine verschlüsselte Verbindung (https) zu erreichen.

Zur Vereinfachung des Benutzererlebnisses wurde ein transparentes Single-Sign-On realisiert, sodass für Benutzer, die sich aus dem Unternehmensnetzwerk anmelden möchten, kein erneuter Login angefordert wird. Dieser Login wird über die Zentrale Benutzerverwaltung (ZBV) der DSV-Gruppe realisiert.

Die Trennung zwischen Applikationsserver und Datenbankserver stellt sicher, dass der Datenbankserver keine unautorisierten Zugriffe über den Webserver erhält. Der Client kann ausschließlich Daten sehen und bearbeiten, die für ihn freigegeben wurden.-

Durch restriktive Hardware-Firewall-Einstellungen (Port-, URL-Einschränkungen) wird der Zugriff auf das System auf das Minimalste eingeschränkt.

B.4 Systemumgebungen

Es gibt eine physische Trennung zwischen der Produktiv- und der Testumgebung mit dedizierten Servern und Umgebungen. Die Testumgebung ist von der Produktivumgebung getrennt, damit die zu testende Software keinen Schaden für den produktiven Betrieb anrichten kann. Die Testumgebung ist der Produktionsumgebung sehr ähnlich, damit Probleme im Zusammenhang mit der technischen Ablaufumgebung bereits im Test erkannt und behoben werden können. Hier wurde ebenfalls ein Testsystem des Zahlungsdienstabwicklers eingebunden. Auf den Testumgebungen sind die Zugriffsbeschränkungen gelockert.

Detaillierte Informationen hierzu sind im Dokument „Architekturbeschreibung und Verschlüsselung“ einzusehen.

B.5 Personenbezogene Daten und Löschung

Detaillierte Informationen hierzu sind im Dokument „Protokollierungs- und Löschkonzept“ einzusehen.

B.6 Nachweise

Das Rechenzentrum von EMMA ist nach ISO 27001 zertifiziert. Das Managementsystem ist nach ISO/IEC 27001:2013 zertifiziert.

B.7 Vertragsverhältnis Mailingwork

Zwischen der S-Communication Services GmbH und der Mailingwork GmbH wurde für die Nutzung und Betreuung von EMMA ein Service Level Agreement (SLA) sowie ein Software as a Service (SaaS) Vertrag geschlossen. In diesem Zusammenhang wurden auch Auftragsverabeitungsverträge gem. DSGVO geschlossen.

Bestandteil dieser Verträge sind auch die Support- und Wartungsbedingungen der Serversysteme einschl. der DR-Instanz, Schnittstellen, Internetzugänge sowie Ansprechpartner und Bereitschaftszeiten inklusive Notfalldienst.

Das Patch- und Releasemanagement ist ebenfalls Bestandteil der o.g. Verträge. Darin wird u.a. geregelt, dass der Softwarehersteller für die Wartung und Weiterentwicklung der Serversysteme von EMMA verantwortlich ist, und in regelmäßigen Abständen Patches auf die Produktionsumgebung der Serversysteme aufspielt. Patches und Releases werden vor dem Rollout auf die produktiven IT-Systeme auf Relevanz geprüft und getestet.

C. Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen

Im Folgenden werden die Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen der Serversysteme sowie der Anwendung beschrieben.

C.1 Infrastruktur

Detaillierte Informationen hierzu sind im Dokument „Architekturbeschreibung und Verschlüsselung“ einzusehen.

C.2 Kommunikationsprotokoll: Transportverschlüsselung

Detaillierte Informationen hierzu sind im Dokument „Architekturbeschreibung und Verschlüsselung“ einzusehen.

C.3 Datenverschlüsselung

Detaillierte Informationen hierzu sind im Dokument „Architekturbeschreibung und Verschlüsselung“ einzusehen.

C.4 Change- und Releasemanagement mit Protokollierung

Es ist sichergestellt, dass durch Modifikationen vorgesehene Mechanismen (automatisierte Berechnungen, Sicherheitsvorkehrungen, Eingabekontrollen, funktionale Abläufe etc.) nicht beeinträchtigt werden.

Changes an der IT-Infrastruktur werden in enger Abstimmung zwischen dem Softwarehersteller Mailingwork GmbH und der S-Communication Services GmbH vorgenommen. Der Softwarehersteller und die S-Communication Services GmbH verfügen über einen etablierten Changemanagement-Prozess.

Changes an der Middleware oder Anwendung selbst werden von der Mailingwork GmbH nach Absprache in die Testumgebung eingespielt, getestet und freigegeben, bevor sie produktiv gesetzt werden.

Changes werden in einer Change-Datenbank dokumentiert und erfordern die Freigabe der S-Communication Services GmbH.

Detaillierte Informationen hierzu sind im Dokument „Architekturbeschreibung und Verschlüsselung“ einzusehen.

C.5 Regelmäßige Penetrationstests der Anwendung

Source Code Scans und Code Reviews werden ca. vierteljährlich durchgeführt und zusätzlich werden jährlich 2-3 Pentests durch Kunden durchgeführt.

C.6 “Restore-Tests, Fail-Over-Tests

Es finden in unregelmäßigen Abständen Restore-Tests und Fail-Over-Tests (min. jährlich) statt. Die Funktionsfähigkeit der Datensicherungssysteme und der Erfolg der durchgeführten Datensicherungen wird regelmäßig kontrolliert (z. B. Prüfung auf Vollständigkeit und Aktualität). Die Fail-Over-Tests dienen

dazu zu prüfen, ob die Disaster-Recovery-Instanz einsatzbereit ist und die Aufgaben des produktiven, aktiven Clusters übernimmt, falls der produktive Cluster in einem Rechenzentrum ausfällt.

C.7 DDoS-Schutz

Die gesamte EMMA Infrastruktur ist gegen DDoS-Angriffe geschützt. Es kommen VPN-Verbindungen und Firewalls zum Einsatz. Im Rahmen der Systemhärtung wird die aktuelle Implementierung und Konfiguration stets u.a. anhand aktueller Erkenntnisse zur Abwehr von Angriffen geprüft und verbessert.

C.8 Anwendung Katastrophen-Fall (K-Fall)

Zur Sicherstellung der Ausfallsicherheit wird eine Disaster-Recovery (DR) Instanz in getrennten Feuerschutzbereichen betrieben. Für den sehr unwahrscheinlichen Fall, dass die produktive Instanz oder die Internetleitung komplett ausfällt, übernimmt die DR-Instanz die Funktion der produktiven Instanz. Zu diesem Zweck werden die Daten redundant in beiden Bereichen gehalten und synchronisiert. Darüber hinaus besteht ein(e) Business-Impact Analyse / Plan.

C.9 Softwaretests

Das Hauptziel der Tests für die Software EMMA ist die Qualität der Software sicherzustellen und eine stetige Weiterentwicklung zu garantieren. Das beinhaltet das Beseitigen etwaiger Fehler, Nachtests und letztendlich die Produktivsetzung. Tests werden vor jedem Release durchgeführt. Neben der Entwicklungs- und Liveumgebung steht für die Tests eine separate Testumgebung zur Verfügung. Testprozesse sind spezifiziert und werden dokumentiert.

C.10 Datensicherung

Eine Datensicherung der Produktionssysteme findet kontinuierlich statt. Alle produktiven Datenbanken sind redundant ausgelegt und regelmäßige Datenschwenks sichern die Datenkonsistenz und Integrität. Detaillierte Informationen hierzu sind im Dokument „Protokollierungs- und Löschkonzept“ einzusehen.

C.11 Monitoring

Es erfolgt eine stetige Überwachung der Systeme mit Hilfe von Monitoring- und Überwachungstools, u.a. mit Eset und Heimdal. Vor der Überschreitung der definierten Schwellwerte werden geeignete Gegenmaßnahmen eingeleitet.