INFORMATION SHEET CLOUD (DSGVO / GDPR)

MMIS-46101

DSGVO Information

Bei der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, kurz „DSGVO“) handelt es sich um eine für alle Mitgliedsstaaten der Europäischen Union verbindliche Gesetzgebung zur Durchsetzung des Grundrechts auf informationelle Selbstbestimmung (vgl. Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union).

Die DSGVO regelt die Grundsätze zum Umgang mit personenbezogenen Daten, hebt also vorwiegend auf das (organisatorische) Verhalten der für die Verarbeitung Verantwortlichen ab. Die DSGVO ist keine Produktnorm und eine entsprechende Zertifizierung ist nicht möglich. Gleichwohl bestimmt Art. 32 DSGVO („Sicherheit der Verarbeitung“) Grundsätze zur Sicherstellung eines angemessenen Schutzniveaus bei der Verarbeitung personenbezogener Daten und Anforderungen an technische und organisatorische Maßnahmen.

Diesen Anforderungen kommt ASC durch eine Vielzahl von Vorkehrungen nach, die sich inhaltlich am IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik orientieren. ASC ist durch den TÜV SÜD – eine der weltweit führenden Zertifizierungsstellen – nach DIN EN ISO/IEC 27001:2017 zertifiziert und erfüllt somit die international wichtigste Norm zur Informationssicherheit. Zusätzlich wurde ASC vollständige Compliance zum U.S.-Standard ISAE-3402 / SOC-2 Type I attestiert.

Das Erfordernis für und die Zulässigkeit von Aufzeichnungen, die Wahrnehmung von Betroffenenrechten sowie die Einhaltung gesetzlicher Aufbewahrungs- und Löschfristen muss der für die Verarbeitung Verantwortliche unter Würdigung seines konkreten Tätigkeitsfeldes stets selbst prüfen, beantworten und sicherstellen. Der Verantwortliche trägt die abschließende Verantwortung für einen gesetzeskonformen Geschäftsbetrieb.

Die von ASC entwickelten Produkte und Lösungen sowie die über die Cloud bereitgestellten Dienste verfügen über alle Funktionen, die vom Verwender zu ihrem DSGVO-konformen Betrieb benötigt werden. Bei den Cloud-Diensten kommen folgende Aspekte hinzu:

- Der Betrieb erfolgt in Microsoft Azure Rechenzentren innerhalb des Europäischen Wirtschaftsraums. Microsoft stellt ein umfassendes Sicherheitskonzept bereit (aktuell > 90 Sicherheitszertifikate), das im Dokument „Microsoft Azure Compliance Offerings“ zusammengefasst ist.
- Die Übertragungswege zwischen diesen Microsoft Rechenzentren und dem Kunden sind nach einschlägigen Standards gesichert und verschlüsselt.
- Die Interaktionen von ASC mit der bereitgestellten Cloud Lösung sind auf Betriebserhaltung und Softwarepflege beschränkt. Sofern in diesem Zusammenhang bspw. Logfiles verarbeitet werden, erfolgt dies auf Grundlage unserer umfassenden technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO und auf Basis einer mit ASC abzuschließenden Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO.

GDPR Information

Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, in short „GDPR“) is legislation that is binding for all Member States of the European Union to enforce the fundamental right to informational self-determination (cf. art. 8 par. 1 of the Charter of Fundamental Rights of the European Union).

The GDPR regulates the principles governing the handling of personal data, i.e. it focuses primarily on the (organizational) conduct of the persons responsible for processing. The GDPR is not a product standard, and a relating certification is not possible. Nevertheless, art. 32 GDPR ("security of processing") lays down principles for ensuring an adequate level of protection in the processing of personal data and requirements for technical and organizational measures.

ASC meets these requirements through a variety of precautions, the content of which is based on the “IT Basic Protection Compendium” of the German Federal Office for Information Security. ASC is certified by TÜV SÜD – one of the world's leading certification bodies – according to DIN EN ISO/IEC 27001:2017 and thus complies with the most important international standard for information security. In addition, ASC has been certified as fully compliant with the U.S. standard ISAE-3402 / SOC-2 Type I.

The requirement for and admissibility of records, the exercise of Data Subject rights and compliance with statutory retention and deletion periods must always be examined, answered and ensured by the Controller himself, taking into account his specific field of activity. The Controller bears the final responsibility for business operations that comply with the law.

The products and solutions developed by ASC and the services provided via the cloud have all the functions required by the user for their GDPR-compliant operation. The following additional aspects are to be considered for cloud services:

- Operations is carried out in Microsoft Azure data centers within the European Economic Area. Microsoft provides a comprehensive security concept (currently > 90 security certificates), which is summarized in the document "Microsoft Azure Compliance Offerings".
- The transmission paths between these Microsoft data centers and the customer are secured and encrypted according to relevant standards.
- ASC's interactions with the provided cloud solution are limited to operational and software maintenance. If, for example, log files are processed in this context, this is done on the basis of ÁSC’s comprehensive technical and organizational measures in accordance with art. 32 GDPR and on the basis of a mandatory Agreement for Data Processing pursuant to art. 28 GDPR.