We record & analyze communications

# Data Privacy Policy

## Table of Contents



Scope of this document: ASC Technologies AG, Seibelstrasse 2-4, 63768 Hoesbach, Germany, as well as such affiliated companies pursuant to § 15 of the German Companies Act (AktG) that are covered by the current scope of the relating ISO certification.

# Data Privacy Policy

## 1. Vision

As a worldwide leading provider of omnichannel recording, quality management and AI based analytics, ASC Technologies AG ("ASC", “We”) provides state-of-the-art solutions for digital communications governance and regards the protection of personal data and information security as elementary components of its corporate strategy and as a voluntary commitment to implementation for the entire ASC Group ("ASC"). ASC's dedicated Policy on Data Privacy therefore places the highest demands on full compliance with the GDPR, BDSG, HIPAA, other relevant laws and official requirements to be able to use technologies such as cloud computing and services based on it itself, but above all to be able to offer them to customers as innovative services. ASC endeavors to always implement its measures in accordance with the current state of the art to ensure the highest possible level of security.

## 2. Mission

This policy establishes the framework for the handling of personal data at ASC and the implementation of a data protection management system (“DMS”) which must be adhered to and complied with in all business activities of ASC. ASC fulfills the requirements of Art. 32 GDPR and relies on established security standards to ensure an appropriate level of protection. The information technology is certified in accordance with DIN EN ISO/IEC 27001 and SOC 2 Type II and is based on the IT baseline protection compendium of the German Federal Office for Information Security. Furthermore, ASC has implemented additional security and data protection measures to ensure compliance with HIPAA requirements.

## 3. Principles

Data protection management system (DMS)

To this end, ASC has implemented a DMS that is comprehensively documented and contains detailed procedural instructions. They serve as guidelines for the implementation of data protection-relevant processes and enable transparent traceability of the measures. ASC has appointed a company data protection officer (DPO), a data protection coordinator (DPC) and an information security officer (ISO) to ensure this DMS. These roles are responsible for the monitoring, control and further development of data protection and information security measures and ensure compliance with GDPR, HIPAA and other relevant legal and regulatory requirements.

Data Protection Impact Assessments (DPIAs)

ASC conducts DPIAs for processing activities that are likely to result in high risks to the rights and freedoms of individuals. This explicitly includes any processing activities involving Electronic Patient Health Information (ePHI). The results of DPIAs are documented and used to inform decision-making processes related to data protection.

Technical and organizational measures (TOM)

In accordance with Article 35 GDPR, ASC has defined technical and organizational measures (TOM), which are implemented, maintained and continuously developed by the IT department, ISB, DPO and DPC. These are, for example

- implementation of secure IT systems
- securing networks and encryption of sensitive data
- regular review and updating of the security measures used.

The TOMs are based on the recognized standards of DIN EN ISO/IEC 27001 and the German BSI IT baseline protection compendium. In addition, these TOMs are specifically designed to meet the security rule requirements of HIPAA, particularly concerning the protection of ePHI, including access controls, availability controls, integrity controls, and transmission security. These measures ensure that personal data and ePHI are effectively protected against unauthorized access, loss or manipulation.

Automated and non-automated processing

The requirements of this policy and the DMS cover all processes in which ASC processes personal data or ePHI of individuals - in particular employees, customers, suppliers or other contractual and business partners - in a fully or partially automated manner (e.g. by means of electronic data processing) in compliance with the GDPR.

These requirements also apply to non-automated processing if personal data or ePHI is or is to be stored in a structured collection that is accessible according to certain criteria (e.g. in paper-based personnel, customer or project files).

Internal audits and controls

The ASC data protection officer and the ASC data protection coordinator carry out regular internal audits and controls, especially of the TOMs. These internal audits serve to systematically review the implementation and

effectiveness of the established data protection, HIPAA compliance, protection of ePHI, and security measures. As part of the audits, potential weaknesses are identified and suitable measures for optimization are introduced. The results of the audits are documented and serve as a basis for further improvements.

Training and awareness-raising
To ensure compliance with data protection and security requirements, ASC employees are regularly trained and sensitized from the outset. The training measures impart practical knowledge of data protection requirements, the definition of ePHI, proper procedures for handling and protecting ePHI, and security guidelines and concrete behavior in specific day-to-day work. In particular, the basic principles according to Art. 5 GDPR are taught, such as the minimum principle or the dual control principle. Continuous awareness-raising measures promote awareness of data protection and data security throughout the company.

Employee Commitment
All ASC employees are obliged to comply with data protection regulations and to maintain confidentiality. This commitment is made in writing and includes careful and responsible handling of personal data, protection of ePHI and adherence to HIPAA requirements. Employees are also expressly instructed to report any breaches or suspected breaches in connection with data protection and data security without delay.

Third-Party Data Sharing
ASC shares personal data exclusively with its third-party service provider, Microsoft Azure. ASC has established contractual agreements with Microsoft Azure to ensure that all data processing activities are conducted in accordance with GDPR, HIPAA and other relevant regulations. These contractual agreements, including Business Associate Agreements (BAAs) where applicable, explicitly address HIPAA compliance for any ePHI processed or stored on Microsoft Azure. Regular audits and assessments are performed by external auditors to monitor ongoing compliance and to address any potential risks associated with third-party data sharing.

Incident Management
ASC maintains an ISO27001 certified incident management policy designed to promptly address and mitigate data protection incidents. In the event of a potential data breach or security incident, ASC commits to informing affected clients within 72 hours, or as contractually agreed otherwise. For incidents involving ePHI, ASC will adhere to the breach notification requirements of HIPAA, notifying affected individuals, the Secretary of Health and Human Services, and in some cases, the media, as required by law. This policy includes detailed procedures for incident detection, reporting, and resolution, ensuring that any disruptions to data security are handled efficiently and transparently. Continuous monitoring and regular reviews of the incident management processes are conducted to enhance the effectiveness of the policy and to uphold ASC's commitment to data protection and information security.

Data Retention and Deletion
ASC retains personal data, including ePHI, only for as long as necessary to fulfill the purposes for which it was collected, or as required by applicable laws and regulations including retention periods for ePHI as mandated by HIPAA. Upon the expiration of the retention period, ASC ensures that personal data is securely deleted. Detailed procedures for data retention and deletion are documented and regularly reviewed to ensure compliance with data protection requirements.

## 4. Continuous improvement

ASC is committed to continually improving the effectiveness and suitability of its DMS by evaluating its effectiveness, addressing deviations, and implementing corrective actions where necessary. Feedback from employees and customers is valued as an important driver for growth and performance optimization.

## 5. Accountability & regular review

ASC Executive Board takes accountability for the effectiveness of the multi-management system and ensures that this Policy on Data Privacy is communicated, understood and applied throughout the organization. All employees are responsible for adhering to defined processes and thus contributing to continuous improvement. The Executive Board regularly reviews the MMS and updates this policy to ensure its continued appropriateness and effectiveness.

## 6. Communication

This Data Privacy Policy is publicly available to internal and external interested parties (“stakeholders”). Requests may be addressed to: data.protection@asc.de.