nordoon

2025

Data Processing

Quick Guide

INTRO

In this guide we provide the documentation of the technical and organizational measures to be taken in accordance with the data protection regulations to achieve the protection level for processing (regarding confidentiality, integrity, availability, and resilience of the systems, as well as the regular review of the measures).This document is designed to meet general legal requirements and is intended to provide a general description that will allow a preliminary assessment to be made of whether the data security measures taken are appropriate to the aspects outlined below.

SCOPE OF DATA PROCESSING

Nordoon extracts data from documents and extracted data might contain personal data. Input data is only stored during processing and extracted data is by default deleted after it is retrieved by the user. If the user so decides, both input data and extracted data can be stored in the Nordoon system for the sole role of quality assurance.

TECHNICAL AND ORGANIZATIONAL MEASURES

Pseudonymization

Pseudonymization defines as the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without additional information. The precondition is that this additional information is kept separately, and that appropriate technical and organizational measures are taken.

Nordoon services do not process any personal data that is extracted from documents and as such does not need to implement pseudonymization.

Encryption

Nordoon ensures that all data is encrypted at-rest and in-transit. At-rest data is stored on Microsoft Azure managed storage services where Microsoft ensures security of the data. SSL encryption is used to encrypt data in-transit from customer to Nordoon and between-services within the Nordoon platform.

Confidentiality

Nordoon stores all the data in managed services provided by Microsoft Azure and located in their data center in Frankfurt am Main for the European customers and Azure East US for the US customers. Physical security is ensured by Microsoft. Virtual access is controlled by 2FA and any access to customer data is logged within the Nordoon app and visible to the customer. Access is possible only with explicit permission from the customer and the individual users.

Integrity

Nordoon ensures the integrity of data by implementing and checking access rights within Nordoon internal services. Compliance is ensured by mandatory code-review. Access to data points is logged within Nordoon services.

Availability

Nordoon services are hosted on Microsoft Azure cloud in Frankfurt am Main data center for the European customers and Azure East US for the US customers. Availability is ensured by Microsoft on a physical level and by the Nordoon SysOp team on virtual level. Nordoon also provides a real-time status monitor of service availability located at https://status.nordoon.ai.

Resilience of the IT systems

Nordoon is hosted on Microsoft Azure, which provides elastic scaling of computer and storage services, when required by clients.

Method for restoring the availability of personal data following a physical or technical incident

Nordoon is implementing SOC 2 and ISO 27001, which also covers incident response management.

Procedures for regularly reviewing, evaluating and evaluating the effectiveness of technical and organizational measures

Nordoon manages information security according to SCO2 and ISO27001 which includes regular review of organizational measures.

LIST OF SUB-PROCESSORS

Company	Location	Service type
Microsoft	Frankfurt am Main (EU Customers) Azure East US (US Customers)	Azure Cloud