Data Processing Agreement
Appendix 1: **Data Protection Concept**

Version: 2.5, 17.08.2023
Contact Person: Matthias Menne, Data Protection Officer, onOffice GmbH

Introduction

Annex 1 outlines the technical and organizational measures according to Article 32 of the GDPR, intended to guarantee the security of the processing activities covered by the contract.

- Providing the online CRM software solution onOffice enterprise
- Hosting websites
- Data imports
- Data transfers
- Email hosting

Many processes are performed on the same IT systems and protected by the same security measures. Each chapter begins with an introduction to these standard security measures, followed by a discussion of their components.

Encryption

Network traffic to and from onOffice enterprise is secured using HTTPS, supporting TLS versions 1.0, 1.1, and 1.2. The certificate was issued by "GMO GlobalSign Inc," Portsmouth, NH, USA.

Websites can be secured with certificates verified by "Let's Encrypt," San Francisco, CA, USA.

Data carriers submitted as part of data imports are encrypted before being returned to the customer.

When sending emails, we use TLS with Perfect Forward Secrecy, provided that the recipient's server supports it.

Confidentiality

Confidentiality of personal data is ensured by only allowing authorized individuals physical or logical access to it.

Entry Control

Unless otherwise stated, all processing takes place in the data center of Telehouse Deutschland GmbH (see Appendix 2).

Entry to the premises is regulated by a contactless identification system, which is constantly monitored by security personnel. Video surveillance is also implemented for additional security. Furthermore, each server room is equipped with its own entry-authorization program.

The backups are housed in designated rooms rented from Telehouse Deutschland GmbH at the Düsseldorf data center, which is operated by Equinix (Germany) GmbH.

It is crucial to mention that the stored data is off-limits to employees from both data centers.

Within the business premises of onOffice GmbH in Aachen, client personal data is stored temporarily, but only if absolutely necessary for internal software testing or data imports. The issuance of keys to employees is strictly controlled and well-documented. Moreover, outside of normal business hours, the premises are protected by an alarm system, which promptly alerts security personnel in the event of any alarms.

To ensure security, data carriers used for data imports are kept in a secure storage area within the company's premises. Detailed written documentation is maintained to track the location of these data carriers. The actual data imports occur on a server housed in onOffice GmbH's Aachen office, specifically within a dedicated server room that benefits from robust security measures, including an alarm system, access logging, and video surveillance.

Access Control

To gain access to onOffice enterprise/smart, it is essential to provide the accurate customer name, an active user's name (who is not blocked), and a valid password. The username and password are not displayed in plain text when entered. A software administrator can determine the frequency at which passwords must be changed. Additionally, the password complexity is automatically evaluated upon entry, and if it does not meet the specified criteria, the password will be rejected.

Access to production systems is limited to authorized personnel and protected through the use of public-private key authentication. When an employee departs from onOffice, their access credentials are promptly removed.

The servers' standard software undergoes regular assessments to identify security-critical updates. Once identified, these updates are promptly applied to the system without causing any disruptions to availability.

The processing of the client's personal data by onOffice GmbH employees only occurs outside of the company's physical location, and it is done to the extent required. The IT security policy that is adhered to within the business premises is also followed in this context.

The monitoring of network traffic is carried out by a firewall that operates on a hardware level.

Access Permission

Within onOffice enterprise/smart, it is possible to limit access to records on a per-user basis. To achieve this, records must be assigned to particular users or groups, and appropriate restrictions must be placed on users' privileges. Additionally, there is a feature available to enable a module that allows users to define read and write permissions for their individual Contact / Property / History records. Users also have the ability to generate a list of the most recently accessed records.

In onOffice enterprise/smart, email mailboxes can be allocated to one or multiple users. Once assigned, the mailbox becomes exclusive to the assigned user(s) and is no longer accessible to others.

Integrity

The integrity of data in onOffice enterprise/smart is ensured by keeping a log of any alterations made to Contacts and Property data. Users with administrator rights can access this log to monitor and investigate these changes.

onOffice enterprise/smart has the ability to support multiple clients, with each customer's data securely stored in its own dedicated database. Accessing data from other customer versions is only possible by logging into a different version and providing the client name, user, and password.

Updates to the codebase of onOffice enterprise/smart undergo extensive testing and are first released to a select group of customers for a few weeks. Once this initial period is completed, the updates are then made available to all customers. Bug fixes are regularly implemented for all customers, either twice a week or immediately in urgent cases.

Email attachments are subjected to virus scanning, and the implementation or evaluation of antivirus protection for other operations is in progress.

Availability

Every night, customer databases are backed up using a comprehensive full backup method. These backups are securely stored in rooms rented by Telehouse Deutschland GmbH at the Düsseldorf data center of Equinix (Germany) GmbH (refer to Attachment 2). Additionally, customer files undergo full backups once a month, as well as incremental backups every night.

With the exception of "Data Imports" and "Data Transfers," all data processing takes place at the Telehouse data center. To ensure data availability, there is an N+1 redundant power supply, fire protection systems equipped with optical / thermal fire detectors and Inergen extinguishing systems, as well as redundant network connections to multiple carriers.

Adequate computing capacity is provided to handle all processing tasks, even in the event of multiple server failures. The customer data is securely stored in a RAID5 system.

onOffice takes proactive measures to safeguard against DDoS attacks by actively participating in the Akamai Prolexic Network. All requests made to onOffice GmbH systems are directed through Akamai servers, which effectively filter out any requests associated with DDoS attacks.

Legality of Processing

Data confidentiality is a stringent requirement for all employees at onOffice GmbH, who also receive regular training on data protection and IT security protocols.

Agreements for data processing have been established with all subcontractors, who undergo thorough suitability evaluations prior to entering into contracts. This practice ensures that confidentiality obligations extend to employees of subcontractors as well.

In the planning of functionalities and processes, the principle of data minimization ("Privacy by Design") is always taken into consideration, reflecting a commitment to prioritize privacy.

Data Protection Management

To ensure data protection, onOffice GmbH follows a comprehensive approach that includes work instructions, agreements, and a range of technical and organizational measures. The effectiveness of this data protection concept is assessed at least once a year, and any required modifications are implemented.

Incident Response Management

The IT systems used for processing undergo constant monitoring to ensure the timely restoration of access to personal data during incidents. Subsequent assessments are conducted to evaluate the need for revisions in the IT security and emergency concepts, as well as the sufficiency of technical and organizational measures and IT infrastructure in preventing similar incidents from occurring in the future.

Data Processing in Third Countries

onOffice utilizes Akamai's Prolexic Network to provide optimum protection against DDoS attacks. In order to ensure this level of security, traffic to onOffice GmbH's systems is directed through servers located worldwide. It is worth mentioning that traffic monitoring takes place in the United States, resulting in the potential processing of personal data outside the EU.

1. The client's IP address
2. The domain queried
3. For non-https secured traffic: the URL

In order to ensure compliance with data protection regulations, onOffice and Akamai have adopted the EU Standard Contractual Clauses, specifically selecting Module 3 (Processor and Sub-Processor) in the June 2021 edition.

A thorough evaluation of the legal landscape in the United States, combined with a comprehensive risk analysis, has been carried out. Based on this assessment, the data controller has determined that no additional security measures are required.