POKESHOT
PEOPLE SOLUTIONS PERFORMANCE

# Pokeshot Security Overview

Updated: 27th of Nov. 2018

The following document provides an overview of the Pokeshot internal and external security measures. Please understand that we cannot disclose every detail of our infrastructure to external sources, since this would present a security risk in itself. This document and the security measures in it are based on suggestions of the Bundesamt für Sicherheit- und Informationstechnik (BSI) - the German federal institution for IT security and information exchange, as well as our privacy officer.

# Table of Content

## 0. Privacy

| Question | Answer |
|---|---|
| How is the implementation of the GDPR organized? | An external privacy officer is responsible for advising on and controlling of GDPR related topics. |
| Name and contact details of the privacy officer: | Jan Wandrey<br>Motzener Straße 25<br>12277 Berlin<br><br>kontakt@agidat.de<br>Tel: +49 30 720102230 |
| In what manner are employees trained for the correct adherence to the GDPR? | Employees get a GDPR instruction, before working with privacy related data. Furthermore, constant sensitization via privacy newsletters, web trainings, and personal consultations with the external privacy officer, will be conducted. |
| Is the processing of privacy related data documented? | There is a register of every process. These processes are checked against the GDPR, to make sure they are permissible. Each process undergoes a risk assessment. |
| Will privacy data be erased? | Yes - as soon as the data is not needed any longer for fullfilling contracts or legal requirements. When the data is gone, a restoration is not possible. |

# 1. IT Organization

| Question | Answer |
|---|---|
| Does Pokeshot have an inventory for storage devices? | Pokeshot keeps track of its hardware by use of an inventory list. Important hardware, such as servers, PCs and storage devices, is labelled for easy identification. |
| Does Pokeshot use encryption methods? | Every storage device is encrypted with industry standard methods. |
| How does Pokeshot reposit storage devices? | Storage devices are either locked away in server or network rooms, which are behind an electronic locking and alarm system, or kept in lockable cupboards within the same security perimeter. Only people who can prove they need them are handed portable storages. Loss of any of the storage devices is reported immediately. |
| Does Pokeshot check storage devices from 3rd parties? | 3rd party storage devices are being automatically checked by industry standard anti malware software, on an isolated device. |
| How does Pokeshot handle data erasure? | Upon end of life, data on storage devices is erased by software in several iterations. After that the storage device is being destroyed physically with magnets and force. No 3rd party is involved. Sensitive printed out documents are only shred by the person that had to work with them. |
| Does Pokeshot use 3rd party software for work purposes? | Yes. Open and closed source software from known and reliable companies. |
| Has Pokeshot established an incident management system? | Yes. Pokeshot provides a helpdesk and support platform, where customers can ask questions and get help with any problems relating to our products and services. The current Service Level Agreement (SLA) can be found here: Service Level Agreement : Pokeshot Helpdesk |
| How is collected data handled by Pokeshot? | Data which is collected for different purposes is being processed and stored separately. Separation takes place logically as well as physically. Meaning: Different machines will handle different data. The same goes for software. |

## 2. Credential Policies

| Question | Answer |
|---|---|
| How does pokeshot handle logins? | Every employee of Pokeshot has an own domain account with a unique password. Before a user gets to login to any service the operating systems asks for separate credentials. Apart from SSO enabled services, every application requires a different account name and password. |
| Is login information stored anywhere? | Yes. Pokeshot uses a reliable and well known digital password vault to store login information. Access to credentials is managed by a handful of account administrators and is checked by them on a regular basis. There are no physical copies of login data. |
| Are password policies in effect? | Yes. Every employee is required to change his or her password at least on an annual basis. Passwords have to be at least 12 characters long and have to contain at least one number and one special character. Whereever possible the use of a Multi-Factor-Authentication is required. Some of the critical services are safeguarded by certificates as well. |
| What happens when an employee leaves the company permanently? | After a controlled handover, all logins and data the employee stored is frozen. Meaning: No access to accounts or stored data of the account is possible, unless all of it is unblocked again. This will only be the case when the same employee is rehired. Per German law, emails are required to be stored for 6 years. After that, they will be erased. |

## 3. Security Solutions

| Question | Answer |
|---|---|
| In what context do employees work on their machines? | Employees work with user privileges. Only administrators can work with permanent admin or root privileges, when this is necessary. Meaning: Any malware that slips through other security layers will only be able to run under limited rights, which prevents this software from spreading further. |
| Is anti malware software used? | Pokeshot is using industry standard anti malware solutions to prevent malicious software to take hold of the firm's systems. These solutions are updated several times a day and are set to automatically scan for threats as soon as files are created or processed. |
| Is a firewall in place? | Yes. Pokeshot uses industry standard firewalls on the WAN as well as LAN side of its network to prevent unauthorized access to the network resources. Every PC and laptop is also secured with a firewall. |
| Connections to Pokeshot networks and services, coming from outside the office are protected? | Yes. Pokeshot uses industry standard encrypted tunnels, as well as certificates and login credentials to secure external access. Wifi access is restricted to company owned devices - which are allowed via a manually maintained white list. The individual MAC address is used for this. Private devices never have access to the internal network. |

## 4. Data Security

| Question | Answer |
|---|---|
| How is data backed up? | Pokeshot backs up crucial data in a on prem hosted cloud and Office 365. Along with other data, these files are backed up on a separate secure hardware storage regularly. Several generations of backups are stored and some of them are held outside the server room in a secure environment and casing, to keep them safe from any disaster. Only industrial standard backup methods are used -> RAID, established archive systems and copy applications. |
| Are backups being tested? | Backups are tested for functionality on a sample basis. |
| Are critical systems being monitored? | Yes. Pokeshot uses internal and external tools to monitor critical services and systems. In case of an outage administrators are informed, so they can take actions in a timely manner. This includes only checks concerning technical availability. Personal or private data is not processed within this framework. |
| Is access to critical data restricted? | Yes. Pokeshot works with individual access rights or groups to prevent or grant access to critical data. Only employees that absolutely need to work with certain data are granted access to it. Critical data is encrypted during transfer and at rest. |
| How is server hardware protected from external influences? | Air conditioning is preventing server hardware from overheating and premature aging. Electricity fluctuations and breakdowns are being intercepted by UPS. In case of a hard drive failure, within the RAID system, the server will give out a message to the administrators, whereupon a quick (hot) swap can be initiated. Various lock mechanisms prevent unauthorized physical access. |

## 5. Premisis Security

| Question | Answer |
|---|---|
| How is the building protected Pokeshot resides in? | The entrance of the building is fitted with a camera system, that provides 24/7 surveillance and is connected to a security company. Same security firm also is on a 24/7 stand-by duty and conducts guard patrol on a regular basis. |
| Is the office itself protected? | Yes. The office entrance is protected by an electronic locking and alarm system, which is connected to motion sensors. This whole arrangement in turn is connected to the aforementioned security company. In case of an emergency, security is alerted and will check the situation. Access to the rooms of the office is only granted to employees with individual transponders. |
| How are server and network rooms protected? | Server and network rooms are situated behind the above mentioned security system. These rooms are locked and will only be unlocked in times of maintenance. External maintenance is only conducted under supervision of authorized personell. All other rooms are locked by Pokeshot employees, when work hours are over. |
| What is the procedure for 3rd party visitors or employees? | All external visitors or personell must identify and sign a guest list, before access to the office rooms is granted. Constant supervision by at least one Pokeshot employee will be ensured. |
| Other security measures? | Technical equipment, when not needed, is stored in lockable metal containers. The whole office is fitted with water, gas and smoke detectors. All fire extinguishers are tested and up to date. |

## 6. Additional Security and Compliance

Additionally to the above mentioned points, Pokeshot is using a row of Microsoft services, which all fall under the following rules.

- Office 365 Trust Center – EU Model Clauses FAQ
- Microsoft Trust Center | Office 365 Security
- Data Encryption in OneDrive for Business and SharePoint Online