Shinobi Legends

https://shinobilegends.com

Date of this document: July 21th 2019

# DATA PRIVACY AGREEMENT AND TRANSPARENCY REPORT

## 2018

*In this document included are the privacy guidelines and descriptions of the used methods to ensure conformity with the EU data privacy regulations*

# TABLE OF CONTENTS

## Contents

# ROLES AND POSITIONS

## General Positions (Staff)

The current persons are noted on the “Staff List” in the village navigation of the server.
Account names / character names are used.

There is no record of personal names stored.

In general terms, there are three major parts:

### SERVER OWNER

Which controls everything from the server hardware up to the software and user management. It is “root”, in Linux terms.

### GAME MAIN ADMIN

Those selected few have full access on the user data on the server (messages, accounts, etc.) in order to maintain any inquiries or problems.

Alias: “Long time Staff”

All user data can be viewed.

### PETITION HANDLER

A petition handler has no access to user data except for petitions outside the server in which email addresses from users may have been entered.

### MODERATOR

A moderator has access to reports in the game admin center where users complain and report comments that violate the site rules.

In this, they see more than the usual user as potential posts from closed areas like user dwellings may have been reported.

They may remove comments that are offensive and issue short term bans based on those.

An automatic filter also does show latest comments that contain swear words (internal word list).

### GAME MASTER

A game master is basically a normal user except comments can be posted without a name to enhance roleplay among users.

Additionally, they can remove comments (i.e. when somebody mistyped).

# Game Design in terms of privacy

The design of the game is that of a roleplaying game (RPG) with aspects of leveling and character customization options.
There are three currencies:

- Gold (easy to get and to spent on daily basis for ingame expenses, lost often)
- Gems (harder to get and spent on rare ingame items and expenses, seldom lost)
- Donation Points (hardest to get and spent on highest value items)

The last currency can be acquired directly by supporting the server (donations via paypal) or by leveling ingame which will also award a smaller amount each time a cycle (level 1 to level 15 and boss kill) is completed.

For the game itself there is no personal data needed. All items and customizations are tied to the character, not to a person.
We don't need any private data for the profile and will not collect it.

The game runs on PHP with a MySQL database backend on an Ubuntu Linux machine.

# GENERAL SETUP AND MEASURES

## Physical Server Setup

Cloud Server at Hetzner in Nuremberg:

- CX21 / 40GB / nbg1-dc3 (referred to as APPLICATION SERVER)
- CX11 / 40GB / nbg1-dc3 (referred to as TEST SERVER)
- CX21 / 40GB / nbg1-dc3 (referred to as DATABASE SERVER)

Shared Web- and Mailhosting in Nuremberg:

- Websites: Forum and Wiki // Mails (referred to as MAIL SERVER)

No user data is stored on the APPLICATION SERVER except for IPs that get truncated according to the latter privacy policies.

User data such as ingame mails and email addresses are stored on the DATABASE SERVER.

Lastly, if you send a message to an SL email address, it gets stored and delivered to the MAIL SERVER)

# PROCESSING RECORDS

| NO | JOINT CONTROLLERS | PURPOSE | GROUP CONCERNED | CATEGORY OF DATA | ADDRESSEE | TRANSFER TO THIRD COUNTRY | ERASURE TIME | TOMS |
|---|---|---|---|---|---|---|---|---|
| **01** | n.a. | Identification and account ownership | Accountholders | e-mail address, last ip, cookie id last logged on date | Server Owner Game Main Admin | No | After expiration of account or self-deletion | Measures according to the safety concept, standard protection level, no special measures required according to risk analysis |
| **02** | | Actions based on rule infringement, sexual content and other reports Providing mail service and chats | Accountholders | Personal ingame messages and chats | Petition Handler Moderator | No | After expiration | No special measures |
| **03** | | Claims and processing of donations | Accountholders | e-mail address, paypal data received and account number ingame | Server Owner | No | Same as PayPal | No special measures |

# GENERAL SETUP AND MEASURES

## Stored Data

We store the following personal data tied to a character:

- Email address (for password recovery and notifications as well as a proof of ownership for the character)
- Cookie ID (for settings while being logged out, the cookie is in your local browser)
- Last IP (for identification matters and violations of game policies as well as ban measures)
- Ingame messages you send (which will be kept up to the expiration settings, not deleteable by sender)
- Ingame Chats messages (which will be kept up to the expiration settings)

If the user does not have bought the ingame “non-expiration” option (“eternal shinobi”), the character will be deleted.
Messages will persist until the content expiration date has been reached and then cleaned up.

Expiration settings can be viewed here:

https://www.shinobilegends.com/about.php?op=setup&c=4-135034

Current copy at the date of this report:

| | CONTENT EXPIRATION |
|---|---|
| Days to keep comments and news? (0 for infinite) | **180** |
| Days to keep accounts that were never logged in to? (0 for infinite) | **3** |
| Days to keep level 1 accounts with no dragon kills? (0 for infinite) | **25** |
| Days to keep all other accounts? (0 for infinite) | **180** |
| Seconds of inactivity before auto-logoff | **3600** |

# GENERAL SETUP AND MEASURES

## Backup and Data restoration

For safety and convenience of users (people tend to let characters expire but want them back later on) we do keep backups.

Those backups are archived on the server and are also copied to a file space in the same data center network to ensure there is no single-point-of-failure in case of hardware failure or otherwise.

The backups contain all physical files on the server which hold no personal data.

If a character expires, there is a copy of his/her base data (Char name, gold, items, game progress etc.) are saved to a file in a /logd_snapshots folder on the webserver.
In this process, the following steps are done automatically:

- Email address is replaced by a salted SHA-512 hash to determine ownership in case of restoral
- User is being sent an email about the expiration and the removal of personal data
- Last IP is removed
- Last ID is removed
- Personal Webpage (optional public display the user can fill) is removed

# OS Level Logging on the servers

The server runs on Nginx and PHP. The mails are being handled by the APPLCATION SERVER (sending) as well as the MAIL SERVER (receiving).

Nginx does have access and error logs in place.

Mails that are sent are (linux-default) briefly mentioned in the syslog with the respective mail status (sent/bounced/etc.)

## NGINX (ON APPLICATION + MAIL SERVER)

The logs contain IP addresses but are not linked to an email address or a user account (not identifiable).

The logs are vital in case of DDOS attacks or the like and are logged with entire IP addresses.

The server uses the module fail2ban which will trace the IPs in case of attacks needs the complete IP to not block entire subnets from accessing the server. In case of dynamic or NAT shared IPs this will result in a large disruption of service (experience from US cable companies who pack thousands on one IP even).

However, the data will not be permanently stored. Daily a script (/usr/local/bin/anonip.py by https://www.privacyfoundation.ch/de/service/anonip.html) will scramble the last 12 bits of the access IP. This will ensure a compromise between IT security for the application and server as well as data privacy.

The logs will be stored in /var/log/apache2 with .log.1 (rotated daily) and will be scrambled by the daily cronjob.

## MAIL LOGS (ON APPLICATION SERVER)

The logs are disabled. Postfix won't log any mail activity.

Mail handling will be done on the MAIL SERVER.

## MAIL LOGS (MAIL SERVER)

The logs there contain the standard logging by Hetzner.

It states the usual information like FROM and TO in the maillog – the mail itself is handled the usual way (delivered, bounced, etc.) and has no special handling at the time of generation.

As all mails are routed through this server, the mail logs contain all data entries for sent or received emails.

# MAIL SERVER SETUP

## STANDARD PROVIDER SETUP

No special rules here, the Hetzner privacy rules do apply.

# GENERAL HANDLING AND PRIVACY RIGHTS

## Rights according to GDPR

You have the following rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

### RIGHT TO BE INFORMED

We will inform you upon request where and how your private data is used.

This paper includes all relevant information. You can always inquire via petition ingame if you have specific question not covered by this document.

### RIGHT OF ACCESS

You can file a petition or email us from the account holder's email with a request to access your data and get a copy if you need to. We will provide you in the form you request within one month.

### RIGHT TO RECTIFICATION

If we have inaccurate data, you can either change it ingame or ask to change it via petition ingame or email us from the account holder's email.

### RIGHT TO ERASURE

If a user decides for his entire account along with all personal data to be permanently deleted (which implies the request never being restorable from a backup), the following actions can be done from the game interface. Manually mailing the admin of the site from the verified email address will also work.

- Option "Permanent Delete" while being logged (on the village sections → Privacy Policy)
- Acknowledging the permanency and reading the explanation of the consequences (character permanently lost)

The game will do the following:

- Email the user about the permanent delete (2 factor auth)
- In the Email, there is the explanation again as well as a generated link (valid 24h) which will commence the permanent removal

If the user acknowledges this and clicks the link, the game will do the following:

- Save the unique character account ID in the table “accounts_never_restore”
- Trigger a character deletion procedure to remove the character from the game (certain items like houses will stay server inventory and now be handled)
- Delete all user mails (sent)
- Delete the character restore snapshot files (if character expired in the past or manual deletion occurred)

In case of backups that are being restored (which is always a manual process and the “accounts_never_restore” will always stay up-to-date) the most recent “accounts_never_restore” table will be kept separately and a script will be invoked that will do:

- Check if any of the IDs in the “accounts_never_restore”-table are present in the backup
- If so, do for those:
- Delete base user data
- Delete all user mails (sent)
- Delete the character restore snapshot files (if character expired in the past or manual deletion occurred)

The last part is in a stored procedure that will be stored in the table itself and can be triggered to clean up. (procedure: “cleanup_privacy_forgotten” in technical terms).

This will check against the table and remove automatically all affected rows.

## RIGHT TO RESTRICT PROCESSING

We currently don’t process your data to improve our services automatically.

In general terms, if we ever will there will be an opt-in agreement if you want to participate.

## RIGHT TO DATA PORTABILITY

Portability means you can extract personal information and account associated information.

We have a module ingame to provide you with these information, go to a village square and click “Data Privacy”.

## THE RIGHT TO OBJECT

You have always the right to object and withdraw your permission to use your personal data for marketing purposes.

Those agreements are optional and you can cancel them at any time.

## PayPal / Donation Handling

PayPal itself saves (due to refund request and other issues) the personal information (aka the email address and name of the sender) in the transaction log.

This information is duplicated to the game server where it is used to provide ingame currency (donation points).

Additionally, we do email a receipt to the donator which is sent by our game server and CC to the administrator account.

Currently, as the information is also available in PayPal, we keep this informational email.

## SSL Encryption and data transfers

Automatic data transfers happen in the following instances:

1. Backups
   Those are mostly done via Snapshots of the machine or the 7-day-rotation of backups by Hetzner. Some are done via SFTP (SSH) and are transferred encrypted to the storagebox within the Hetzner data center. No outside line is used.
2. Webserver Traffic (aka access from the outside via browser)
   All standard http is redirected to https and SSL encrypted. SSLLabs are currently giving us an A+ mark for having the highest standards (no weak ciphers accepted etc.).
3. Admin Access to server
   This is done exclusively via SSH and is encrypted.
4. Emails being sent
   The APPLICATION SERVER has dkim, spf and dmarc setup as well as locally encrypted TLS. However, we cannot guarantee all mailserver are accepting TLS, so we cannot guarantee privacy here.
   (Hence we never mail passwords)

# Emails from the server and storage

Mails from the server fall into the following categories.

### REGISTRATION EMAILS AND NOTIFICATION EMAILS FOR THE USER BOUND TO THE ACCOUNT

These emails are not stored by the server nor sent to the server owner.

The TO information is stored, but no link to a user account is being made.

### PETITIONS THE USER CREATES (INGAME WITH ACCOUNT OR OUTGAME WITH NO ACCOUNT)

Petitions can be ingame (then the communication will remain ingame) or outgame (not being logged in / not a user).

In the first case, all mails are retained and handled like any other game mails.

In the second case, communication will be initially by the server (sent through the game), but IF the user replies the reply will be to admin@shinobilegends.com or petitions@shinobilegends.com (ALIAS for the first mail).

Refer in the second case second way to the next block.

### MAILS FROM AND TO ADMIN@SHINOBILEGENDS

These mails are stored using IMAP technology in specific mailboxes respectively.

Handling is done by the server owner (no other access rights for anybody).

These mails will be handled manually, after an individual discussion or case is closed and it is (depending on the conversation) not needed to be kept, the conversation will be deleted.

This applies in all cases – if the “right to be forgotten” is triggered, the mails (if not being legally forced to keep) will be deleted manually be the server owner.

They are exempt from any backup.

# CONTACT INFORMATION & CONTROLLER

## Contact information

Oliver Brendel
Paul-Strian-Str. 8
91301 Forchheim
Germany
admin@shinobilegends.com
https://shinobilegends.com