Alexander Wiener, Dennis Sima, Paul Maurovich, Florian Freimüller, Lucas Walter

ScanBuyGo Technical and Organisational Measures

GDPR Art. 5

Technical and Organisational Measures

Alexander Wiener, Dennis Sima, Paul Maurovich, Florian Freimüller, Lucas Walter

Table of Contents

Technical and Organisational Measures

Alexander Wiener, Dennis Sima, Paul Maurovich, Florian Freimüller, Lucas Walter

Introduction

This document lays out Measures to be taken by ScanBuyGo's Team and Partners in order to protect sensitive data. It is separated into sections for production and development, explaining further measures to be taken throughout the product's active development and maintenance.

Technical and Organisational Measures

Alexander Wiener, Dennis Sima, Paul Maurovich, Florian Freimüller, Lucas Walter

Production Measures

Introduction

This section aims to lay out how to handle potentially sensitive information in ScanBuyGo's production environment including but not limited to customer data or payment information.

Technical Measures

Encryption in transit

Any and all traffic to and from the ScanBuyGo Application Servers is encrypted using modern cryptography. Examples for modern and safe encryption include TLS 1.2 or greater (commonly referred to as HTTPS) or SHA-256 encryption.

Encryption at rest

Data stored on ScanBuyGo Systems, aside from other access control measures, is stored at rest, meaning no data can be read from a hard drive without authorization. This includes encrypting hard drives, using a TPM (Trusted Platform Module) and its functions wherever possible and encrypting sensitive data at the application layer using a hashing function like SHA-256 or bcrypt.

Data minimization

Only as few data as is required shall be processed or stored. In any case, the data stored or returned shall only be as much as is absolutely required to fulfill a purpose or provide the user a better experience.

Password requirements

Any staff or administrator password in any internal or external systems needs to meet the following requirements:

- More than 8 characters
- No common or easily guessable password (e.g. Password123)
- Contain at least one number
- Contain at least one special character

The best and most secure passwords exceed these requirements. It is encouraged to use a password generator whenever possible.
Passwords must be changed if they might have been compromised or guessed.

Technical and Organisational Measures

Alexander Wiener, Dennis Sima, Paul Maurovich, Florian Freimüller, Lucas Walter

Logging

Wherever possible, any access to ScanBuyGo Applications is logged. These logs are to be reviewed weekly for any anomalies suggesting potential breaches of confidentiality. Log data is only retained for 14 days in accordance with the privacy policy.

Organisational Measures

Principle of least privilege

The principle of least privilege is to be considered when setting or handling permissions. Any user, employee or administrator shall only have access to as little data and as few systems as absolutely necessary. To assure this, permissions need to be audited on a regular basis, removing any unnecessary access.

Purpose limitation

Any data that is stored or processed shall only be used in accordance with and for a purpose outlined in the Procedural Directory and Privacy Policy Documents.

Physical device security

Any work devices used to access customer data need to fulfill security requirements in order to protect stored data on them:

- The device shall be locked whenever not in use.
- The device shall not be used in a public area
- The same device/user/container shall not be used for private or unrelated purposes.
- Whenever possible, the entire or sections of the drive in use shall be encrypted.

Hardware Tokens and Multi-Factor Authentication

Whenever possible, any alternative or addition to passwords should be preferred or used. This may include government-issued certificate signatures, one-time tokens or hardware tokens.

Customer support

Customer support shall be able to assist customers with their inquiries without compromising their security or causing a breach of confidentiality. Therefore, while assisting a customer:

- The customer’s identity needs to be confirmed: This can be done either by requesting entered personal data from them such as a full name, address and birthdate or by confirming their email address. Before it is assured that it is the actual customer no data shall be revealed and no account changes shall be made.

- Passwords shall not be reset by support agents: There is a secure way to request a password reset requiring an email to be sent to the customer via the application. If a user requests to have their other personal data edited or appended this can be done but only after confirming their identity.

Working with third parties

Whenever working with a third party, be it an employee, partner or provider, required contracts including proper confidentiality clauses shall be signed and stored even after the collaboration has ended.

No local copies of data

Whenever handling customer data, it shall be avoided to copy and store it locally. If this is required, the local copies shall be removed after use.

Development Measures

Introduction

As ScanBuyGo is in constant development and will require to be maintained to compete with other products in the market appropriate measures need to be taken in order to protect customer data and the product.

Technical Measures

Use anonymized or mocked data for testing

Do not use data from real customers for testing whenever avoidable.

Use secured connections and devices for programming

Use a separate device, user or container for development that is not used for other purposes. For connecting to development environments and code sharing services use secured connections like HTTPS, SFTP or SSH.

Technical and Organisational Measures

Alexander Wiener, Dennis Sima, Paul Maurovich, Florian Freimüller, Lucas Walter

Use a separate testing environment

Use a dedicated, fully separate environment for testing the application. It shall not have any connection to a database, server, etc. used in production and shall not have actual customer data stored in it.

Code Reviewing

Merges between branches require the entire team (respectively Frontend or Backend Team) to approve a pull request. Furthermore, no comments can be open while merging. This is to ensure the entire team is on the same page and to prevent harmful code from being pushed into production.
It is recommended to adopt pair programming in addition to this to provide and receive code feedback while programming.

Organisational Measures

Only deploy to production environments from the master branch

Any deployment into production needs to come from the master branch. This ensures that if it is a feature it has been reviewed 2-3 times by the entire team and that no unapproved development code can end up in a release build, potentially leaking data.

Code sharing

Code may only be shared between team members in internal communication systems. These systems are:

- Azure Repos
- Microsoft Teams

Only program in safe areas

Shoulder Surfing and other attack vectors shall be avoided by only using work devices and programming only in areas where not many people are around. Details about features and database structures shall not be shared outside the team.

Password requirements for developers

Any staff or administrator password in any internal or external systems needs to meet the following requirements:

- More than 8 characters
- No common or easily guessable password (e.g. Password123)

- Contain at least one number
- Contain at least one special character

The best and most secure passwords exceed these requirements. It is encouraged to use a password generator whenever possible.
Passwords must be changed if they might have been compromised or guessed.