DekoEko Security Overview

Infrastructure and Marketplace

“Security that is top of mind”

March 20, 2018

Information Security Officer

| Krakow, Poland | Amsterdam, Netherlands

NOTICE: This document is provided for informational purposes only. It represents DekoEko’s current practices as of the date of issue of this document, which are subject to change without notice. The purpose of this document is to answer common questions regarding internal security matters such as physical security, network security and information security processes of the DekoEko platform.

1 Overview

At the time of this document's publication, DekoEko customers have used our platform to make few thousands transactions, offer more than 3000 upcycling products, and make more for sustainability than ever. And with our global customer base increasing 50% year over year -- those numbers are only going to rise.
Not to mention that processing such a massive amount of purchasing transactions, while simultaneously managing other sustainable initiatives, requires a robust platform that is architected, not just for scalability and performance, but for protection, privacy, and security.
So, as an industry-leading Upcycling Marketplace that is heavily relied upon by high-performance organizations and flagship consumer brands to create, sell, and implement the best sustainable practices, DekoEko is highly differentiated from others in both the engineering and design of our platform architecture, structured upon key functional elements that include:

- ❏ Ease of Use
- ❏ Innovation
- ❏ Collaborative
- ❏ Sustainability-First
- ❏ Transparency
- ❏ Security in Depth

And while each of these principles rank as "high-priority" for consumers when procuring a new business partner in upcycling, perhaps the most important, but least discussed when thinking about upcycling and sustainability, is platform security.

Specifically, DekoEko features a modern, cloud platform operating in a multi-tenant SaaS (Software as a Service) environment, which means DekoEko takes away from customers the burden of maintaining and securing platform used for sustainability. For customers, this means no additional hardware or software costs to consider, no databases to configure, no operating system requirements, and no versions to maintain or update. And because security is top of mind for our team, we follow a "Security in Depth" approach for our Software Development Lifecycle (SDLC), code deployment practices, security patches and backups, architecture and infrastructure, executing across multiple layers of validated security management practices, backed and based on ISO 27001.

In the pages that follow, our Security Management team outlines DekoEko Information Security Management processes and practices, detailing how our team goes to great lengths to protect and secure the integrity, availability and confidentiality of our customers' data.

At DekoEko, security is top of mind, so you have peace of mind.

2 SaaS Platform - Complete Cloud Security

The DekoEko marketplace is architected on a modern SaaS platform. For customers, this means that all of our applications and data is delivered via the Internet and hosted in secure data centers by a third-party, cloud services provider - Amazon Web Services (AWS). AWS' data centers deliver a highly scalable cloud computing platform with high availability and dependability. It is very difficult and expensive to properly secure on-premise data center. Cloud data

center (Amazon AWS) that is being used by DekoEko delivers superb resiliency, cybersecurity and compliance that meet world's top standards. With a cloud-hosted solution, like DekoEko, security responsibilities are shared between our Information Security team and AWS.

For example, AWS is responsible for securing the underlying infrastructure that supports the cloud (e.g. security of the cloud), whereas DekoEko is responsible for anything we store or process in the cloud and/ or connect to the cloud.

Amazon AWS is responsible for protecting its global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS cloud services. As detailed in their documentation for consumers, security is a top priority.

> *"Protecting this infrastructure is AWS's number one priority, and while you can't visit our data centers or offices to see this protection firsthand, we provide several reports from third-party auditors who have verified our compliance with a variety of computer security standards and regulations…"*[1]

Hence, AWS reports like SOC-3 or SOC-2 from independent, third-party auditors are available via AWS' websiat: https://aws.amazon.com/compliance/soc-faqs/

Amazon Web Services Security Whitepaper: https://aws.amazon.com/compliance

The AWS global infrastructure is designed and managed according to security best practices, as well as a variety of industry-recognized security compliance standards. As such, DekoEko selected AWS for our cloud-hosting provider because AWS provides the most rigorous physical and environmental security standards designed to accommodate the needs of high growth enterprise organizations worldwide. Further, AWS has designed its systems to tolerate system or hardware failures with minimal customer impact.

So, as the AWS customer, we know we're building web architectures atop some of the world's most secure computing infrastructure. Nevertheless, we still make it a priority to manage information security internally with equally high standards so our customers enjoy complete cloud security.

3 DekoEko Information Security Management Systems (ISMS)

3.1. Information security organization

DekoEko knows complexity and criticality of information security and its governance demand the highest organizational levels. As a critical resource, data is treated like any other asset essential to the survival and success of an organization - yours and ours. To enable secure business operations, DekoEko has implemented an effective security governance strategy approved by our Management Board.

1

As part of our security governance strategy, DekoEko has appointed Information Security Officer which includes function of Data Protection Officer.

3.2. Information security standards and compliance

DekoEko attaches significant importance to information security and compliance, as reflected by our security organizational structure and our internal management practices. For example, DekoEko focuses on continuous development and refinement of our information security management practices, in accordance with industry standards and trends. Detailed policies, procedures, and instructions have been developed and put in place to define the roles, tasks and permissions of both employees and coworkers, in addition to the involvement and management of any third parties that participate in execution and delivery of our business processes.

Specific to compliance, DekoEko adheres to and complies with relevant legalities, contractual requirements and latest industry-standards, including:

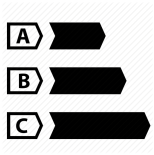
- ISMS based on ISO 27001
- Applications tested to OWASP standards
- EU PII legislation (GDPR - General Data Protection Regulation)

3.3. Security Controls and Practices

Asset Management

The process of asset management is crucial to information security and business operations, and includes information and the information-processing environment. Accordingly, DekoEko established internal policies, procedures and instructions to identify, implement, maintain, and optimize security of assets. Every asset is owned, employees are trained to understand their responsibilities, and procedures are aligned with security standards to keep assets secure.

Classification of Information



Another practice strictly implemented is the classification of information - one of the most important parts of information security management and, simultaneously, one of the most complicated. For managing this practice, DekoEko implemented a four step process to classify all company information. This process includes the following: inventory tracking, classification, labeling and handling.

Risk management

DekoEko' Information Security Management System obliges us to regularly review assets the company possesses and to classify them against three dimensions: probability of threat occurrence, possible consequences and level of protections. The sources of the threats can include natural disasters, technical failures, legal obligations (compliance), and human activities (malicious and non-malicious).

Information Security Awareness

Apart from various technical security protections, DekoEko believes cybersecurity starts with consciousness of our employees. This consciousness is ingrained at all levels of the organization. Our employees participate in the following programs:

- PII management
- Compliance (ISO 27001, GDPR, etc)
- Techniques of secure software development
- Social engineering prevention
- Related industry security programs and training

Recruiting Process

DekoEko pays special attention to the verification and hiring of our employees. Depending on the personnel function, coupled with the legislation of the country in which a vacancy is being created, DekoEko takes appropriate actions, such references checks, among other measures, to verify the integrity of the person who would join the team.

Onboarding and Exit

DekoEko onboarding process contains employee review and acceptance of data privacy agreements, non-disclosure agreements, mandatory security trainings, access setup to the systems, and other related items necessary for creating a secure and reliable work environment. Each new employee is required to complete the onboarding process before permissions and access to confidential data (where applicable) are granted.

The exit process is designed to prevent an exiting employee from accessing or acquiring confidential data or any other asset that belongs to the company during their departure, whether departing voluntarily or exiting as result of termination. Depending on the position within the organization, DekoEko organizes and secures knowledge transfer to ensure that key responsibilities are not lost.

New Employee Procedures and Policies

Every new employee, before starting their official duties, must pass cybersecurity and personal data processing security trainings. These trainings contain a mandatory knowledge check. Additional mandatory requirements instruct every employee to sign a non-disclosure agreement that intends to protect and secure proprietary company secrets and customer data.

Audit Program

DekoEko has implemented a continuous audit testing program according to ISO 27001. Internal audits test and optimize system operations and organizational processes. Specifically, these audit programs focus on:

- Software development
- HR/Administration
- Customer Support

- Sales and Marketing
- Business Operations
- Infrastructure Access Rights
- Vulnerability Scans
- Backups Audit
- PII Security
- Other related processes.

Antivirus and Malware Protection

Every employee is obliged to use antivirus on workstations and mobile phones/tablets. DekoEko policy of using antivirus software on hardware and infrastructure is monitored and audited.

Usage of Subcontractors

DekoEko does not outsource its operations to subcontractors.

3.4. Protection of Data

Denial-of-Use Control

DekoEko takes appropriate security measures to protect against any unauthorized use or access of our hardware and systems. Our security infrastructure includes Intrusion detection services, security monitoring, restricted physical access, restricted network access, encrypted data access, firewalls, isolated public/private LANs and real-time antivirus. Further, as part of our ISMS, we maintain an Access and Password Policy, which requires periodic password updates and enforces monitoring of password guidelines.

Data Transmission Control

Transmission-sensitive data between DekoEko and a user's browser is encrypted using at least 128-bit data encryption. AWS server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt our customers' data. Communication between users and the DekoEko platform is secured by HTTPS. Data backups are transferred also encrypted with very limited access.

Separation Control

All DekoEko customer data is encrypted and secured in a similar fashion - using a multi-tenant structure. The data is segregated using a dedicated authorization engine, with another layer of separation delivered by AWS.

Data at Rest

Data at rest is encrypted and the encryption keys are protected using AWS Key Management Service (KMS). AWS KMS is a managed service to create and control the encryption keys used to encrypt data, and uses Hardware Security Modules (HSMs) to protect the security of keys. AWS Key Management Service is integrated with several other AWS services to help protect data at rest. AWS Key Management Service is also integrated with AWS CloudTrail to provide logs of all key usage, which help meet regulatory and compliance needs.

Data at Transit

DekoEko ensure a high level of security by implementing newest cryptographic protocols that provide communications security. HTTP access is protected via protocol TLS 1.2 - the newest version of that protocol.. A full list of cipher suites that are currently in use in TLS 1.2 is listed below:

ECDHE-ECDSA-AES128-GCM-SHA256

ECDHE-RSA-AES128-GCM-SHA256d

ECDHE-ECDSA-AES128-SHA256

ECDHE-RSA-AES128-SHA256

ECDHE-ECDSA-AES256-GCM-SHA384

ECDHE-RSA-AES256-GCM-SHA384

ECDHE-ECDSA-AES256-SHA384

ECDHE-RSA-AES256-SHA384

AES256-GCM-SHA384

AES256-SHA256

Data Retention Periods

Data is stored no longer than required by GDPR and Accounting regulations.

3.5. Monitoring and Response Management

Information Security Incident Management

In the event of a security incident, DekoEko has implemented and tested procedures it follows, with special care for emergency incidents. Whenever an incident concerns customers data or equates to a security breach, our international support team informs customers as soon as the breach is formally detected and according to timeframes outlined in our Incident Management Policy.

Security Logs

Marketplace logs are kept at minimum 3 months. System and audit logs are kept a minimum 1 year. Stored logs are secured, such that no single person is able to delete all backup copies. Retention policy refers to 9 types of logs pushed daily to KMS encrypted S3 bucket.

3.6. Identity and Access Management

Rights & Roles Matrix - Segregation of Duties

DekoEko security system is based on execution of the 'Segregation of Duties' principle, which attempts to prevent a single individual from access and authority of executing two or more conflicting sensitive transactions that have the potential to significantly jeopardize security of the company's assets. On top of this principle and in alignment with any identified risks, the security

team of DekoEko has built a Rights & Roles Matrix that provides information on access levels of various functions to the company's assets (including PII of our customers).

Multitenant Architecture

Like most SaaS companies, DekoEko platform architecture is structured on a multi-tenant system. Within this structure, there are several architectural protections that provide top security for each tenant. Separated by an authorization engine, separation is supported by multiple test scenarios that are automatically verified before a general release of any new version of the platform.

Internal Authentication

Authentication and authorization are crucial elements of platform security, and supports the strict implementation and monitoring of our internal Password Policy. As such, passwords have termination dates, minimum length and minimum complexity parameters and differ per system and account. Privileged accounts are managed separately as high risk points. No shared accounts are used anywhere in the DekoEko platform.

SSO

DekoEko has implemented a broadly supported industry standard for Web SSO – SAML 2.0. This standard not only allows for quick setup and configuration, but is also supported by a majority of Identity Providers on the market.

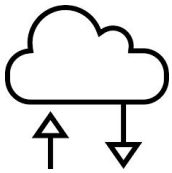
3.7. Physical and Environmental Security

Because DekoEko is hosted by AWS, no data is stored on our site, nor does our staff have physical access to servers and network equipment. Terms and Conditions of AWS services guarantee compliance with industry-standard security requirements. Specifically, physical access to Amazon AWS data centers is enforced and controlled by AWSs' electronic access control system, featuring responsible and sophisticated technical and physical controls designed to prevent unauthorized access. Please refer to https://aws.amazon.com/security

Physical access by DekoEko personnel within our regional offices is monitored. DekoEko facilities are equipped with fire detection and suppression systems, security cameras in CCTV system, backup generators for back office servers.. Internal policies include storage device decommissioning, secure disposal for equipment data and media.

Transmission Protection

Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations enforcing the flow of information to specific information system services. ACLs, or traffic flow policies, are established on each managed interface, and accordingly manage and enforce the flow of traffic.



Network Monitoring and Protection

DekoEko actively monitors its platform on both the network and application level. Apart from the monitoring provided and maintained by DekoEko team, the network is also monitored by AWS staff. AWS utilizes a wide

variety of automated monitoring systems to provide a high level of service performance and availability. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.

3.8. Business Continuity Process and Disaster Recovery (BCP&DR)

AWS infrastructure offers a high level of availability and provides DekoEko features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact. Data center Business Continuity Management at AWS is under the direction of the Amazon Infrastructure Group. Data centers are built in clusters in various global regions.

3.9. Third-Party Cooperation

DekoEko platform cooperates with the third-party sub processors for some functions. These include:

FreshMail: This sub-processor powers the email campaigns for newsletter subscribers.. The content of that emails is created by the DekoEko and can include PII of subscribers (e.g. First Name, e-mail address, etc.).

AWS Amazon: Data center

Stripe and Płatnosci24: This sub-processors provide online credit card payments services. Those services can be used by the customer in the DekoEko platform for processing marketplace purchase transaction