# Priva Information Security whitepaper

This Information Security whitepaper provides a general overview of the information security measures taken by Priva.

This is a public document in order to provide clarity to Priva's customers and partners by being transparent on which security measures are implemented and managed within Priva. In case of additional questions, please contact Priva's Security, Quality and Compliance (SQC) team via sqc@priva.com.

## 1. Organizational security

Priva has a Strategic policy, which is the foundation for the other policies and thus provides direction for further implementing information security and quality within Priva. It defines the purpose, contents, structure, objectives, responsibilities, and the management of the policies.

In order to provide such a level of continuous operation, Priva has implemented an Integrated Management System (IMS) in line with the International Standards for Information Security(ISO/IEC 27001), and Quality Management (ISO/IEC 9001). Note: This security whitepaper focuses on information security. The IMS also provides a clear overview of all the security measures and, moreover, the IMS is a useful tool to continuously improve Priva's security posture. Priva employs strict policies and procedures by taking into account the confidentiality, the integrity and availability of Priva's systems and services.

### 1.1 Compliance

Priva has a dedicated Security, Quality and Compliance (SQC) team in order to make sure Priva complies with the applicable standards. They determine what controls, processes and measures are needed to meet these standards.

Priva complies to the following standards related to information security and privacy:

- ISO / IEC 27001 – Information Security Management
- GDPR compliant

### 1.2 Employee background checks

To ensure that employees and contractors are suitable for the roles for which they are considered, Priva has set guidelines for pre-employment screening. Priva has taken into account that there must be a justified cause and that the screening is necessary in order to verify whether someone's profile and someone's past records meet the desired confidentiality and integrity levels for a specific role within Priva. Until the screening is successfully performed, the employee is not assigned to their role.

### 1.3 Security awareness

Apart from IMS related responsibilities, there are trainings for all employees and contractors within Priva (end users). The Security, Quality and Compliance (SQC) training hosted by the Priva Academy is an obligatory training for every employee or contractor who works for Priva. A part of the SQC training is security awareness. It is required to successfully complete the SQC training periodically. The knowledge of the employee will be tested based on tests. The employee needs to have sufficient knowledge on the security principles of Priva in order to successfully pass the training. Additionally,

there are some roles which receive additional security awareness sessions based on their security clearance.

### 1.4 Dedicated Information Security team

Priva has a dedicated Information Security team, as part of the SQC team. The Information Security team is responsible for implementing and coordinating the security initiatives. This team develops and implements corporate information security and privacy policies and related documents. Additionally, this team develops processes in order to manage information security within Priva. They have a consulting role in Priva-wide projects to advise diverse teams about security risks and how to manage these risks.

## 2. Physical security

### 2.1 Priva offices

Priva controls access to their offices and facilities with the help of access cards, locks and alarms. Priva provides access to employees and contractors based on their 'need-to-know' for a specific role. Visitors will be guided through the facilities. The Human Resource (HR) department assigns employees and contractors to specific roles. The Hospitality department manages the access to offices and facilities of Priva. They also periodically review the assignment of access cards. Access at Priva facilities is controlled by alarm systems to detect on unauthorized physical access, as well as fire protection utilities.

### 2.2 Priva's Corporate Main Equipment Room

At its Corporate Main Equipment Room (MER), Priva takes the responsibility for the physical security, power, cooling and storage. Access to the servers in the MER is restricted to authorized personnel. Any other access is only allowed after approval of respective managers and needs to be guided by authorized personnel. The area is protected with appropriate access controls to protect this area from unauthorized personnel.

### 2.3 Priva Cloud services

For Priva Cloud services, the Microsoft Azure Cloud is used. Microsoft Azure is a Cloud platform that offers a high level of security as confirmed by the over 90 compliance certifications it holds. These certifications are listed on Azure's compliance documentation website. Detailed information on Microsoft's security measures can be found at the Microsoft Trust Compliance Center.

On top of Microsoft Azure, we have developed our Priva Cloud services. Microsoft Azure provides us with secure data centers, secure physical infrastructure and standard components. This means Priva can focus on secure software design, secure coding and secure configuration of our Cloud services. During the development and use of these services, we apply well-known security principles, such as 'security by design' and 'defense in depth'.

Our Architects and Security Specialists work closely with the development teams, so that information security is an integral part of the development process. During development, we continually test whether our products and services meet the required security level. This is done using risk assessments, automated tests and manual code reviews, in line with our software development policy and other information security policies.

To assure Priva (Cloud) services are secure, Priva also hires independent ethical hackers to perform periodic pen tests (penetration tests). Findings are investigated and resolved so that the security

level is increased continuously. When a service or hardware device is adequately protected, the ethical hackers provide a TPM (Third Party Memorandum) to formally confirm their findings about the security level. In addition, Priva is ISO9001 and ISO27001 certified.

# 3. Infrastructure security

## 3.1 Network security

Priva's network security and monitoring provides multiple layers of protection and defense. Firewalls are used to protect the network from unauthorized access and malicious traffic. The firewall activity is monitored and strict working procedures apply. Furthermore, firewall changes will follow the change management procedure with a formal approval. Priva deploys network segmentation to protect its systems and information. For development practices a test environment, separated from the production environment, will be used . The infrastructure and applications are monitored for suspicious activity and checked for any (technical) vulnerabilities. Notifications are triggered if there is abnormal or suspicious activity in Priva's environment.

## 3.2 Network redundancy

All critical components of Priva's environment and services are highly available. Priva uses multiple routers, gateways and switches to ensure redundancy on device-level. This prevents Priva's internal network from having single points of failure.

## 3.3 Intrusion detection and prevention

Intrusion detection and prevention mechanisms are used for critical systems or servers of Priva. Logging is used for administrative access and system calls on production servers. For Azure production resources Privileged Identity Management (PIM) is implemented for the privileged access rights in order to perform privileged commands. Moreover, multi-factor authentication is enforced on all Priva accounts.

At the Internet Service Provider (ISP), a multi-layered security approach is used. It includes network routing, rate limiting and traffic filtering.

## 3.4 Hardening of servers

Servers are hardened before going into production, for example by disabling unused functions and network ports and by changing default passwords. Additionally, all servers are provided with the same operating system image and consistent group policies before they go in production.

# 4. Data security

## 4.1 Security by design

Every change needs to follow the change management procedures of Priva. Security aspects are assessed and considered prior to a change. Also within projects security will be considered upfront. Additionally, Priva has a Software Development policy with strict policy statements on security aspects.

## 4.2 Secure software development

Within the Software Development process automated tests are used to automatically test the software requirements. These software requirements are set before the coding starts. The automated tests also check for vulnerabilities in the code. Besides the automatic testing, all software code is subject to a code review. Priva uses a Development, Test, Acceptance, Production (DTAP)

phased approach. The code will be tested for security requirements during code reviews, using automated code analysis tools and by external penetration testing.

### 4.3 Data encryption

All confidential data transfers within the network are encrypted in transit using Advanced Encryption Standard (AES) 256 encryption algorithms and Transport Layer Security (TLS 1.2). Encryption is employed as a means of better ensuring data integrity via restrictions on who can manipulate data via ability to: read, write, modify or execute (r/w/m/x). Priva maintains the passphrases or keys used for encryption and decryption.

- **Data-at-Rest** – Encryption for data at rest is provided on Azure Storage, where Microsoft controls the encryption and keys. All storage accounts used are encrypted.
- **Data-in-Transit** – All data in transit over public networks shall be encrypted. HTTP over TLS (HTTPS) or VPN has to be enabled.
- **Local Hard Drives** – Local HD encryption ensures the security of sensitive data stored on local hard disks for workstations.

### 4.4 Data retention

Priva does not retain data longer than necessary for the purposes for which they are processed. If the Agreement with customers is terminated, Priva shall promptly return or destroy at the request of the customer all confidential information of the customer (please also refer to the general Terms and Conditions).

For personal data Priva adheres to the General Data Protection Regulation (GDPR) and does not retain data longer than for the purpose for which this data is processed unless the data must be kept longer in order to comply with legal obigations, such as a statutory retention period. For more information on personal data, please refer to Priva's Privacy Policy.

## 5. Identity and access control

### 5.1 Multifactor authentication

Multifactor authentication (MFA) is enforced for all Priva employees and contractors. For customers of Priva cloud services, MFA is enforced by default. It is highly recommended for customers to use MFA. It provides an extra layer of security by requesting an additional verification factor in addition to the password.

### 5.2 Access

Priva adheres to the principles of 'least privilege' and 'need to know' for access and permissions to systems and information. Access rights can only be granted if there is a formal request with respective management approval. Additionally, access rights will be periodically reviewed.
Access to Priva's production environment is governed by Privileged Identity Management (PIM) and as such is managed 'just-in-time'. Access to systems, applications etc. is logged and monitored.

## 6. Operational security

### 6.1 Vulnerability management

Priva has a dedicated vulnerability management process. There is also a Vulnerability Management procedure prescribing the set of important rules and considerations of vulnerability management. Priva uses automated third-party scanning tools and penetration testing by external security firms. The vulnerabilities are frequently assessed and discussed by Priva security specialists. Vulnerabilities

are managed and prioritized based on the risk. Vulnerabilities are tracked until they are remediated by either patching the vulnerable systems or applying relevant other controls.

## 6.2 Logging and monitoring

Priva monitors and analyses information gathered from services and usage of assets. This information is recorded in the form of event logs, audit logs, fault logs, administrator logs, and operator logs. These logs are automatically monitored and analysed to a reasonable extent that helps identify anomalies such as unusual activity in employees' accounts or attempts to access information. The logs are stored in a secure server isolated from full system access, to manage access control centrally and ensure availability. Priva's cloud services are monitored and disruptions will be noted on the Priva Status Dashboard. To monitor the different logs, various systems are being used with automated alerting based on alert criticality.

## 6.3 Malware protection

Detection, prevention and recovery controls to protect against malware are implemented. Servers and workstations within Priva are automatically updated with malware protection. Priva uses automated scanning of systems to stop malware from spreading to the Priva network. Priva also uses third-party detection tools in order to identify malicious traffic, like phishing and spam. Priva's employees and contractors are also required to complete the SQC training where they are trained on security awareness including how to recognize phishing and malware and how to report it at Priva.

## 6.4 Backups and restore

Priva creates backups of physical servers, virtual servers, databases, configurations of switches and routers and appliances on a daily basis. Backups are stored locally and are copied to the cloud on a daily basis. Restore is done on a regular basis in test environments. In production environments a restore is performed if needed.

## 6.5 Disaster recovery and business continuity

Application data is stored on resilient storage that is replicated across data centers. At the data centers there are power back-up, temperature control systems and fire prevention systems as physical measures to ensure business continuity. These measures help Priva achieve resilience and redundancy. Priva has a disaster recovery plan which describes the procedures in case of a disaster or emergency.

## 6.6 Endpoint security

All workstations are run on an up-to-date OS version and are configured with anti-virus software. All activities will be logged and monitored and monitoring systems will provide automated alerts. These alerts are handled by IT and Information Security specialists. Workstations are configured in line with Priva's standards for security. All stations are required to be configured, patched and tracked according to Priva's workplace management practices. Priva has developed and implemented operational and technical information security policies in which endpoint security is also addressed. Priva mobile workstations are configured to protect data at rest by using Full Disk Encryption. Moreover, a complex password policy is enforced. Based on these policies, strong passwords and multifactor authentication are also technically enforced.

# 7. Security incident Management

## 7.1 Incident response

Priva has an implemented Security Incident Management procedure. Incidents will be tracked and appropriate corrective actions will be taken if needed. The procedure also outlines the responsibilities of all parties and external communications. In addition, Priva will perform root cause analyses to implement (additional) controls to prevent recurrence of similar events.

## 7.2 Data breach

Priva has an internal data breach policy and a data breach reporting procedure which is in line with the GDPR. Priva notifies the concerned Data Protection Authority (Autoriteit Persoonsgegevens) of a breach within 72 hours after notification of the breach, in line with the GDPR. Depending on specific requirements, Priva notifies the customers as well if necessary. As data processors, Priva informs the concerned data controller(s) without undue delay in case of a data breach.