Famly ApS: Overview of Security Processes

October 2015

Please consult **http://famly.co** for the latest version of this paper

Table of Contents

1. INTRODUCTION TO SECURITY AT FAMLY 3

2. PHYSICAL SECURITY 3

2.1 PHYSICAL AND ENVIRONMENTAL SECURITY 4
2.2 FIRE DETECTION AND SUPPRESSION 4
2.3 POWER 4
2.4 CLIMATE AND TEMPERATURE 4
2.5 STORAGE DEVICE DECOMMISSIONING 4

3. TECHNICAL SECURITY 5

3.1 SECURE NETWORK ARCHITECTURE 5
3.2 SECURE ACCESS POINTS 5
3.3 TRANSMISSION PROTECTION 5
3.4 NETWORK MONITORING AND PROTECTION 6
3.5 FIREWALL 6
3.6 DATA TRANSFER 6
3.7 DATA STORAGE SECURITY 6
3.8 DATABASE SECURITY 6
3.9 DATA BACKUP 7
3.10 DATA DURABILITY AND RELIABILITY 7
3.11 FAMLY AVAILABILITY AND PERFORMANCE 7
3.12 PATCHING AND SECURITY UPDATES 7
3.13 EU SERVER CENTER COMPLIANCE 7
3.14 LOGIN AND PASSWORD SECURITY 9

4. ORGANISATIONAL SECURITY 9

4.1 AUTHORIZATIONS 9
4.2 CONFIDENTIALITY 9
4.3 LOGGING 10

1. INTRODUCTION TO SECURITY AT FAMLY

At Famly we are focussed on security in all that we do. We do not only do what is necessary from a legal and regulations perspective, but go beyond with further securing our operational setup and our apps. This page describes just some of the measures we take internally as well as how our server operator Amazon Web Services go the extra mile to keep data secure. Famly's setup run on infrastructure in Frankfurt that is so secure that it is used by both governments, healthcare and payment providers as well as financial services. We make sure that our customers' and users' data is safe at all times both in transit and at rest.

The following will cover Famly's:

- Physical Security
- Technical Security
- Organisational Security

2. PHYSICAL SECURITY

Famly's servers are located in **Frankfurt, Germany** within the EU Union and are run by Amazon Web Services (AWS). AWS is one of the largest and most secure data center providers in the world. It is guaranteed that our customers' and users' data will never leave Germany. AWS provides multiple availability zones within the Frankfurt region. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains. In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers.

2.1 Physical and Environmental Security

AWS's data centers are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. All physical access to data centers by AWS employees is logged and audited routinely.

Famly's offices are protected with fire detection as well as electronic security and intrusion alarms. No customer data is stored at Famly's offices or on local employee computers. All data is accessed from Famly's offices via secure encrypted connections with the data center.

2.2 Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

2.3 Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

2.4 Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. Management AWS monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

2.5 Storage Device Decommissioning

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to

unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

3. TECHNICAL SECURITY

3.1 Secure Network Architecture

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 to enforce the flow of information to specific information system services.

ACLs, or traffic flow policies, are established on each managed interface, which manage and enforce the flow of traffic. ACL policies are approved by Amazon Information Security. These policies are automatically pushed using AWS's ACLManage tool, to help ensure these managed interfaces enforce the most up-to-date ACLs.

3.2 Secure Access Points

AWS has strategically placed a limited number of access points to the cloud to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API endpoints, and they allow secure HTTP access (HTTPS), which allows Famly to establish a secure communication session with our storage or compute instances within AWS.

In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with Internet service providers (ISPs). AWS employs a redundant connection to more than one communication service at each Internet-facing edge of the AWS network. These connections each have dedicated network devices.

3.3 Transmission Protection

Famly connects to an AWS access point via HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery. For an additional layer of network security, Famly uses Amazon Virtual Private Cloud (VPC), which provides a private subnet within the AWS cloud. Authorized Famly personnel

connects to the AWS data center using Secure Shell (SSH). Secure Shell is blocked by the firewall by default, and is only temporarily opened for a specific IP for debugging or maintenance purposes. Such events are logged with information about when, who and why.

3.4 Network Monitoring and Protection

Family utilizes a wide variety of automated monitoring systems through AWS 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.

3.5 Firewall

EC2 Security Groups together with VPC are used to only allow connections to instances on ports specified in the configuration. For example webservers are protected in such a way, that only connections originating from the Elastic Load Balancer (ELB) and targeting a specific port are allowed. That means no one can connect directly to the Web Servers.

At the Famly office Famly personnel connect to the Firewall via wire to avoid eavesdropping. Devices utilizing Wi-Fi connect to the Firewall via industry standard AES WPA2-PSK. The Wi-Fi password is rotated regularly. No ports are opened for incoming traffic and UPnP is disabled.

3.6 Data Transfer

All data transferred to and from Famly's users and our servers are encrypted with a 256-bit SSL certificate with extended validation (EV) from Thawte. Thawte is one the the leading SSL certificate providers worldwide. Famly has gone through an extensive verification process in order to receive the certificate. All data transfers to and from Famly's mobile and browser apps are encrypted with this 256-bit certificate. All internal data transfers between Famly's servers are protected by VPC - a secure and logically isolated portion of the AWS infrastructure.

3.7 Data Storage Security

Famly uses Amazon Web Services S3 storage. Amazon S3 Server Side Encryption (SSE) uses one of the strongest block ciphers available – 256-bit Advanced Encryption Standard (AES-256). With Amazon S3 SSE, every protected object is encrypted with a unique encryption key. This object key itself is then encrypted with a regularly rotated master key. Amazon S3 SSE provides additional security by storing the encrypted data and encryption keys in different hosts.

3.8 Database Security

Famly's data is stored in an industry standard AES-256 encrypted database. All Famly's data is synchronously replicated securely between multiple zones in the Frankfurt, Germany region for

high durability and availability. Furthermore, the database is backed up fully once every day. Between the daily full backups, a by-the-second incremental backup is maintained.

3.9 Data Backup

Famly ensures that data stored on Famly's platform is backed up at all times down to the second. Famly both uses full as well as incremental backups. Famly regularly makes restore-tests of former completed backups to ensure that the backup works as intended.

3.10 Data Durability and Reliability

Amazon S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 region. To help provide durability, Amazon S3 PUT and COPY operations synchronously store data across multiple facilities before returning SUCCESS. Once stored, Amazon S3 helps maintain the durability of the objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

3.11 Famly Availability and Performance

To improve availability Famly utilizes a multi-server setup that spans all the availability zones in the Frankfurt, Germany region. Famly's multiple webservers are located behind an Elastic Load Balancer (ELB). This ensures that the web-tier does not have a single point of failure. If a server fails for whatever reason traffic is automatically routed to the remaining healthy servers and a new server is automatically booted, installed and eventually replaces the failed server.

If the load on the web-tier increases above a certain threshold EC2 auto-scaling ensures that more servers are booted, installed and eventually becomes part of the web-tier and thereby decreases the load. When the load falls below a certain threshold, servers are automatically decommissioned.

3.12 Patching and Security Updates

Famly utilizes as many managed services at Amazon as possible. This means that Amazon handles all security upgrades, patches and backups. Amazon's expertise and massive scale ensures that Famly always runs on up-to-date and security patched environments. The parts of Famly's setup that cannot utilize AWS Managed Services, are clearly described in internal documentation, and are extensively monitored and patched regularly.

3.13 EU Server Center Compliance

Amazon Web Services Compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud. Amazon is approved in accordance with the EU Data Protection Directive. This is the Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (also known as Directive 95/46/EC). Broadly, this Directive sets out a number of data protection requirements, which apply when personal data on EU citizens is being processed. AWS certifications and assurance programs further include:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA
- DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

Further information on compliance available at https://aws.amazon.com/compliance/
Further information on AWS security available at https://aws.amazon.com/security/

3.14 Login and Password Security

Very few authorized Famly personnel has access to Famly's administration account at AWS and all logins require two-factor authentication and are extensively logged.

To access Famly you will need a username and password. The password needs to be of a certain password strength. All login attempts are logged with detailed information. A user can change password and this triggers an automatic message to the registered users email with information about the password change.

4. ORGANISATIONAL SECURITY

4.1 Authorizations

All employees in Famly who have access to personal data are authorized by Famly. Such authorizations indicate the access and for what purposes the individual employee has been given access to. Famly's employees are only authorized to access the customers' personal data for operational or technical purposes. Famly's employees do not have access to personal data that is not covered by their authorization. The number of employees at Famly with this authorization is kept to a minimum.

Famly verifies and updates authorizations continuously. Such authorizations will be adjusted or cancelled when an employee changes position, responsibility or resigns.

Famly's platform is set up so that the customer can authorize its employees based on roles with different permissions and rights. Other users of the solution must also be subject to authorizations that provide appropriate access. All new and revoked authorizations are logged.

4.2 Confidentiality

All employees of Famly that may have access to personal data are in their employment agreements subject to confidentiality.

Confidentiality is also maintained by Famly after the termination of Famly's agreement with the customer. Famly employees are covered by confidentiality obligations even after their termination.

4.3 Logging

All access to personal data in connection with the use of Famly's platform is automatically logged. The logging includes IP-address, time, username, type of use and the person the data pertains to.

Should Famly access personal data based on a support or technical request from the customer, then this access is logged as well.

If you have any questions regarding our security feel free to contact security@famly.co