



BlackFog, Inc.

Technical and Organizational Measures

Revision: April 3, 2024

Table of Contents

Access Control	2
System Access and Access Control	2
Measures to Establish Integrity	4
Data Availability & Resilience of the Systems.....	4
Data Protection Management.....	5
Privacy by Design and Privacy by Default.....	6

Access Control

BlackFog does not own, lease or operate any BlackFog server infrastructure for its offices or production environment. The BlackFog production environment is a purely cloud-based infrastructure hosted in AWS data centers throughout the world. BlackFog has access control measures in place to prevent unauthorized access to data processing equipment where personal data is stored or processed.

System Access and Access Control

BlackFog relies on the following system access control measures to prevent unauthorized persons from using data processing systems where personal data is stored or processed.

Network and Hardware Security

BlackFog uses a role-based security architecture and requires that users of the system be identified and authenticated before they can use system resources and implements mandatory multi factor authentications (MFA). Resources are protected by native security and add-on software products that identify and authenticate users and validate access requests against users' authorized roles in access control lists.

All resources are managed on a tenant basis and each resource is assigned an owner. Owners are responsible for approving access to the resource and performing checks on access by role. Employees may only access the system through a 2048 bit certificate based SSL protocol and only designated managers have access to the underlying operating system through dedicated certificates using the SSH protocol.

BlackFog maintains a SOC that monitors critical systems and alerts around the clock to manage security incidents. These services are operated in a compliant and data protection-friendly manner while ensuring a threat response that is appropriate to the organization's risk level. Access rights are continually reviewed by team leaders and reconciled with the job description, tasks to be separated, and risks associated with access rights.

Only authorized persons can access systems that process personal data. BlackFog uses multiple authorization levels when granting access to systems. All employees access BlackFog's corporate systems via a personalized account (user ID) and have access only to the systems they need to access to perform their duties. Authorizations and privileges are reviewed on a regular basis. Similarly, rights to access systems are reviewed when employees are assigned new roles or leave BlackFog.

Hiring ("Onboarding") and Departure ("Offboarding") of Employees

When an employee is hired, he or she is assigned to a position in the HR management system. 10 (ten) days before the employee's start date, the HR team creates a so-called "onboarding" ticket that contains the employee's user IDs and the access rights to be granted. The ticket is used by the IT service desk to create user IDs and access rules. The access rules are defined according to the minimal principle (each employee is granted only the permissions he/she

needs to perform his/her task). In addition, the ticket system contains a template for employees who change their position and the associated rights, which must be changed accordingly within the existing access rules.

Access rights are reviewed as required by team leaders to determine if they need to be revoked. When evaluating access rights, team leaders consider the job description, the tasks to be separated, and the risks associated with access rights.

After an employee's employment ends, the IT Service Desk removes the employee's access in all systems. The IT Service Desk uses the tickets to lock user IDs and delete all access roles from IDs owned by the ticket's employee.

Data Access Control

BlackFog controls access to systems containing personal data through a mixture of role-based access control (RBAC) and user rights management. This ensures that access to and use of data is minimized, both in terms of general processing and in terms of the list and scope of access for BlackFog employees. These access controls vary depending on the sensitivity of the data stored and operational requirements.

Data Separation

Networks are segregated and segmented. This works within RBAC to minimize risks in line with sound security and data protection practices. For example, data for different products/purposes are processed separately where possible, including by separating production and test environments. Where appropriate, data is processed separately to avoid unnecessary mixing of data and processing beyond the purpose.

Data Anonymization

BlackFog anonymizes data wherever possible and data is not identified by customer name unless necessary or requested specifically from customers directly.

Measures to Establish Integrity

Transfer Control

BlackFog has forwarding controls in place to ensure that data is secure during transmission and that the level of protection does not fall below a minimum standard once it leaves the perimeter.

These security measures include securing transmissions with SSL/TLS, https, etc. and the use of Anti Data Exfiltration (ADX) throughout the organization. BlackFog maintains firewalls and other standard security systems to protect operations and data.

Firewall systems are in place to filter unauthorized incoming network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network Address Translation (NAT) functionality is used to manage internal Internet Protocol (IP) addresses. Administrative access to the firewall is restricted to authorized personnel.

Data Input Control

BlackFog has audit controls in place to log who has accessed or modified personal data, including linking such controls to individual accounts.

Data Availability & Resilience of the Systems

BlackFog creates backups of critical data in accordance with common practice and ensures that these backups act as a reliable failover in the event of a catastrophic failure.

Customer data is backed up and monitored by Operations staff for completeness and exceptions. In the event of an exception, Operations performs troubleshooting to identify the root cause and then reruns the backup job immediately or as part of the next scheduled backup job, depending on the preferences specified by the customer in the documented work instructions.

The backup infrastructure resides on private networks that are logically secured from other networks.

BlackFog monitors the utilization of infrastructure, both internally and for customers, to ensure that service delivery meets service level agreements.

BlackFog evaluates the need for additional infrastructure capacity in response to the growth of existing customers or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- CPU Utilization
- Disk Capacity
- Network Bandwidth
- Database Load

BlackFog has implemented a patch management process to ensure that contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and BlackFog system owners review proposed operating system patches to determine if the patches are applied on a weekly basis.

BlackFog is responsible for determining the risk of applying or not applying patches based on the security and availability impact of these systems and any critical applications hosted on them. BlackFog staff will verify that all patches have been applied and that a reboot has been performed, if applicable and according to availability standards in place.

Redundancy is built into the system infrastructure that supports the data centre services to ensure that there is no single point of failure, which includes firewalls, routers, and servers. If a primary system fails, the redundant hardware is configured to take its place.

Data Protection Management

BlackFog maintains a variety of privacy policies and procedures for which the DPO (Data Protection Officer) and BlackFog management are ultimately responsible. BlackFog continually updates its privacy and security measures in accordance with updated policies, applicable laws and best practices. This includes regular reviews of documentation of procedures, training, and technical and organizational measures, maintaining and creating processing logs, and conducting data protection impact assessments as appropriate.

BlackFog has processes, policies and procedures that describe security, logical access, computer operations, change control and data communication standards. Teams can only access systems using these mandatory protocols and procedures.

Employees are bound to confidentiality agreements as a condition of their employment.

After termination of the contractual relationship, the data will be deleted in accordance with data protection and the principles of data minimization will be taken into account.

Subprocessor

BlackFog ensures that all sub-processors comply with the relevant security and data protection standards and that these requirements and obligations are included as part of the GCU.

In the case of long-term cooperation, there is an ongoing review of the sub-processor and its level of protection.

Incident Response Management

BlackFog has processes and tools in place to respond to security and other incidents, including firewalls, anti data exfiltration systems, and collaboration between the DPO and Threat Management department.

There is a documented process for detecting and reporting security incidents/data breaches (particularly with regard to the obligation to notify the supervisory authority) and a documented process for dealing with security incidents. Insofar as data processed on behalf is affected, a process ensures that the incident is immediately reported to the client, i.e., the controller as defined by the GDPR.

Security incidents and data breaches are documented and there is a formal process with assigned responsibilities for follow-up and implementation of any resulting actions.

Privacy by Design and Privacy by Default

Personal data is collected and processed only to the extent necessary for the prescribed purpose. Data subjects have a simple way to exercise their rights.

Data protection principles are already observed during software development. In particular, employees are encouraged and trained to implement technical and organizational measures as part of product development that ensure compliance with the requirements of the GDPR and specifically the rights of data subjects. The software is designed in such a way that the amount of data collected as well as the scope of processing is limited to the extent necessary. Insofar as various settings options exist within the software, the setting in which the smallest possible amount of personal data is processed is always selected in the delivery state.

Quality assurance tests and results are documented and maintained along with the corresponding change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents these approvals.

Version control software is used to manage source code versions and migrate source code through the development process to the production environment. Version control software maintains a history of code changes to support rollback capabilities and tracks changes for developers.