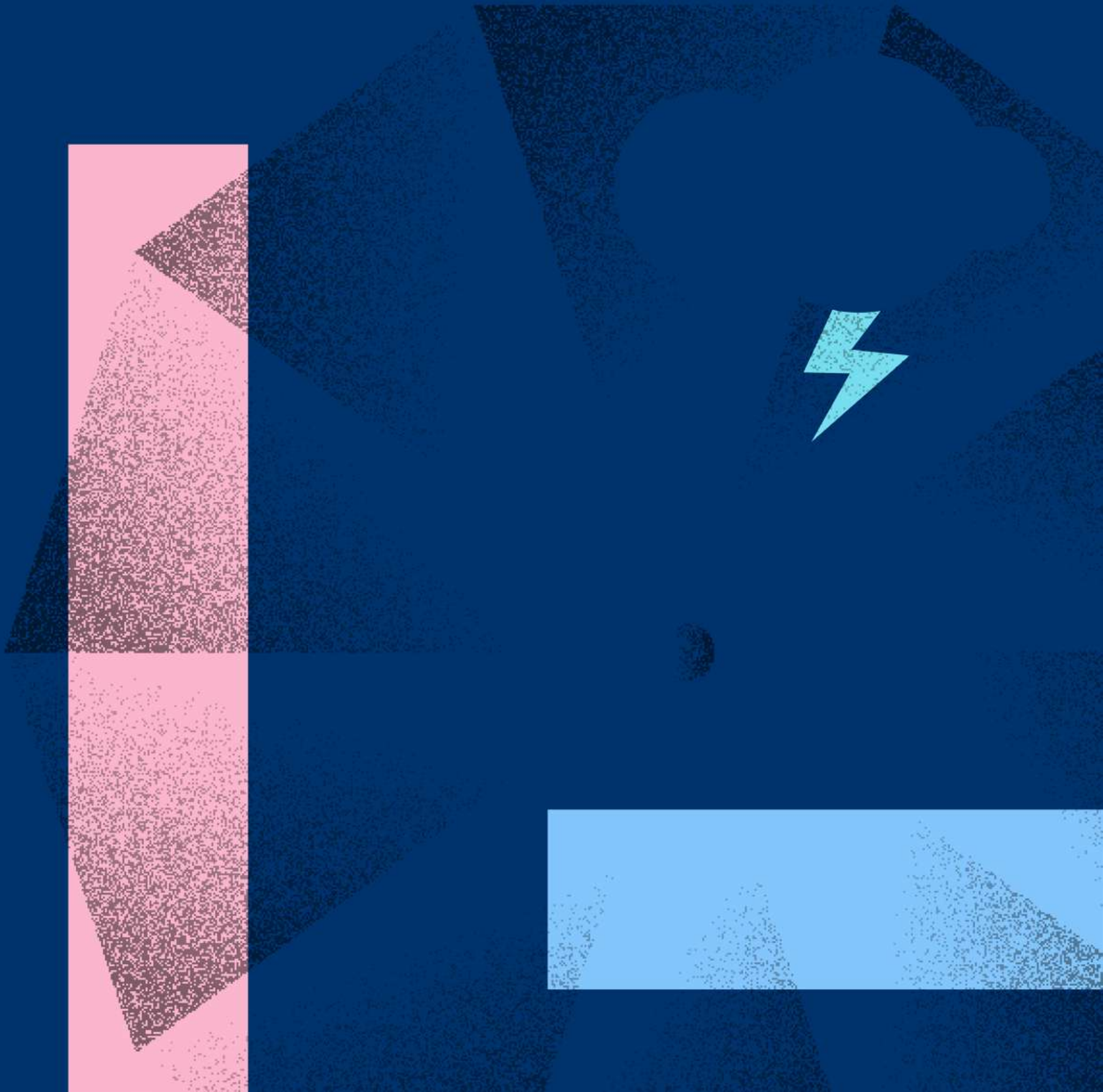
productiMe

Business Continuity And Disaster Recovery Policy



Secure Data Storage, Backup, And Recovery

Productive supports your agency's business continuity and ensures full recovery of your data in the least possible time so that your business operates without interruptions.

BACKUP POLICY

Data entered into Productive is regularly backed up. All backups are encrypted and stored at an offsite location to help ensure that they are available in the unlikely event that a restore is necessary.

DAILY BACKUPS

As an extra precaution, Productive regularly takes automatic database snapshots, which we securely move to a separate data center in case of a regional AWS failure. Our database snapshots are stored for 30 days.

At Productive we perform two types of manual database snapshots. We perform short-term backups once every 3 hours and store the data for 2 days. This is done to ensure that the least possible amount of data is lost in the case of an unfortunate event. We perform long-term backups once every few months and save the data in cold storage for an indefinite period of time. We have a standby replica of the database in case something physically happens to the original one. Everything is backed up in real time to make sure that your data is safe.

Productive is responsible for performing regular backup and disaster recovery tests to ensure a recovery and business continuity plan in the case of a natural disaster or failure. Our system is closely monitored 24/7. In case anything happens, Productive knows about it immediately and can react. There are real-time reports in place that ensure we are ready to fix any issue.

Files uploaded to Productive as attachments are not backed up on the same schedule, and instead rely on Amazon S3's versioning mechanism and their claimed 99.999999999% durability. Files associated with Productive tasks from a supported cloud storage provider are also subject to the storage provider's own backup procedures and policies.

SERVER ACCESS AND LOCATION

To ensure your business continuity and protect your business against major disruptions such as cyber-attacks, natural disasters or supply failures, Productive is hosted entirely on Amazon Web Services (AWS), which is hosted in Europe (eu-west-1).

The precise location of AWS data centers is known only to Amazon employees who have a legitimate business need to have such information. Amazon provides a highly secure architecture and restricts unauthorized access to their systems.

We use multiple independent systems to provide load balancing (Enterprise Load Balancers, or ELB service), compute power (Elastic Compute Cloud, or EC2 service), scalable and redundant databases (Relational Database Service, or RDS) and storage (S3, EFS and Glacier).

We use multiple independent AWS services in order to achieve:

- Load balancing - Application Load Balancer (ALB)
- Computing - Elastic Compute Cloud (EC2), Elastic Container Service (ECS)
- Scalable and redundant databases - Relational Database Service (RDS)
- In-memory queues and caching - ElasticCache
- Storage - Simple Storage Service (S3)
- Content delivery - CloudFront

PHYSICAL SECURITY

AWS is well known for its highly controlled data centers worldwide. AWS offers a robust physical security program with multiple certifications, including an SSAE 16 certification. A number of physical controls are in place to prevent any kind of unauthorized access. To learn more about AWS data storage, backup and recovery, please visit: https://aws.amazon.com/security/

Response In The Event Of A Disaster

AVAILABILITY AND RESILIENCY

Productive has designed redundant systems to keep its services running even if some parts of underlying infrastructure experience issues. Productive services are configured in such a manner so as to withstand long-term outages to individual servers and availability zones. Using AWS infrastructure, all data in Productive is replicated in multiple geographic regions to ensure high level of durability in the case of a disaster.

DISASTER RECOVERY

Productive targets a Data Recovery Point Objective (RPO) of 3 hours for at least 7 days, and up to 24 hours beyond 7 days. Due to the distributed nature of Productive services, RTO for systemic disasters involving data recovery is targeted at 8 hours.

NOTIFICATION AND COMMUNICATION

Productive has established internal communications using industry standard security protocols so that our staff and management will be notified instantly during any emergency event, or when any data recovery plan is initiated or deactivated.

DISTRIBUTION, RELOCATION, AND REMOTE WORK

In case of an emergency or disaster, Productive staff will follow policies and use tools and equipment that enable independent and distributed remote work. If Productive’s primary work location is inaccessible or unavailable, all staff will work from home or at an alternate work venue.