ANNEX III – CHILI publish SECURITY POLICY

Version: 01 August 2022

Our customers trust CHILI publish with their data, and this responsibility is something we take seriously. We take appropriate security measures to ensure our customer and business data is protected.

Data center and network security

We ensure the confidentiality and integrity of your data with industry best practices. CHILI publish primarily hosts Service Data (as defined below) in Microsoft AZURE data centers that have been certified as ISO 27001, PCI/DSS Service Provider Level 1, and/or SOC 2 compliance. See https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/ and https://docs.microsoft.com/en-us/azure/security/ for more information.

Application security

We take steps to securely develop and test against security threats to ensure the safety of our customer data. In addition, CHILI publish employs third-party security experts to perform detailed penetration tests on different applications within our family of products. This according to formalized procedures.

Product security features

We make it seamless for customers to manage user access. All communications with CHILI publish servers are encrypted using industry standard HTTPS over public networks, meaning the traffic between you and CHILI publish is secure.

Compliance

We use guidance of general accepted security and privacy frameworks to help our customers to meet their own compliance standards. CHILI publish is ISO27001:2017 certified.

You can find the Certificate itself and The Statement of applicability at
https://www.chili-publish.com/trust/

Data Center Physical security

Facilities

CHILI publish hosts Service Data in Microsoft AZURE data centers that have been certified as ISO 27001, PCI/DSS Service Provider Level 1, and/or SOC II compliance.
https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure

Microsoft AZURE infrastructure services include back-up power, HVAC systems, and fire suppression equipment to help protect servers and ultimately your data.

On-site Security

Microsoft AZURE on-site security includes several features such as security guards, fencing, security feeds, intrusion detection technology, and other security measures.

CHILI publish nv
Korte Keppestraat 9, Box 11
9320 Erembodegem - Belgium
info@chili-publish.com
+32 (0)2 888 65 11
VAT BE 0825.827.712

Service Data
Service Data is any information, including personal data, which is stored in or transmitted via the CHILI publish services, by, or on behalf of, our customers and their end-users.

User Data
User Data covers user account and subscription data (incl. contract details, credentials, permissions, …). User data is stored at rest in the Azure Germany West Central Region in Frankfurt.

Support Data
Support Data means the data Customer provides to CHILI publish on the support platform. Support Data is stored within Europe.

Data Hosting Location
CHILI publish leverages Microsoft AZURE data centers in different regions. The Customer can select a data center in a region, offered by CHILI publish (see Annex V – Data centers).

Network security

Protection
Our network is protected through the use of key AZURE security services, integration with protection networks, regular audits, and network intelligence technologies which monitor and/or block known malicious traffic and network attacks.

Architecture
Our network security architecture consists of multiple security zones. More sensitive systems, like database servers, are protected in our most trusted zones. Other systems are housed in zones commensurate with their sensitivity, depending on function, information classification, and risk. Depending on the zone, additional security monitoring and access controls will apply. DMZs are utilized between the Internet, and internally between the different zones of trust.

Third-Party Penetration Tests
In addition to our extensive internal scanning and testing program, each year, CHILI publish employs third-party security experts to perform a broad penetration test of key CHILI services.

Intrusion Detection and Prevention
Service ingress and egress points are instrumented and monitored to detect anomalous behavior. These systems are configured to generate alerts when incidents and values exceed predetermined thresholds and use regularly updated signatures based on new threats. This includes 24/7 system monitoring.

DDoS Mitigation
CHILI publish has architected a multi-layer approach to DDoS mitigation. The use of Microsoft AZURE scaling and protection tools provide deeper protection along with our use of Microsoft AZURE DDoS specific services.
Logical Access

CHILI publish nv
Korte Keppestraat 9, Box 11
9320 Erembodegem - Belgium
info@chili-publish.com
+32 (0)2 888 65 11
VAT BE 0825.827.712

Access to the CHILI publish Production Network is restricted by an explicit need-to-know basis, utilizes least privilege, is frequently audited and monitored, and is controlled by our Operations Team.

Security Incident Response

In case of a system alert, events are escalated to our teams providing Operations, Network Engineering, and Security coverage. Employees are trained on security incident response processes, including communication channels and escalation paths.

Encryption

Encryption in Transit

All communications with CHILI publish UI and API's are encrypted via industry standard HTTPS/TLS (TLS 1.2 or higher) over public networks. This ensures that all traffic between you and CHILI publish is secure during transit.

Encryption at Rest

Service Data is encrypted at rest in Microsoft AZURE.

Availability & continuity

Uptime

CHILI publish maintains a system-status, which includes system availability details, scheduled maintenance, service incident history, and relevant security events. Uptime identifies the availability of the services excluding scheduled maintenance.
Scheduled maintenance is maintenance that might include downtime and is planned and communicated beforehand:

- 3-5 business days in advance: send out a notification to inform about the scheduled work, its purpose, and foreseen outage's
- At the completion of the changes confirming the maintenance is finished and the actual downtime taken

Redundancy

CHILI publish employs service clustering and network redundancies to eliminate single points of failure. Our strict backup regime allows us to deliver high level of service availability, as Service Data is replicated across availability zones.

Disaster Recovery

Our Disaster Recovery (DR) program ensures that our services remain available and are easily recoverable in the case of a disaster. This is accomplished through building a robust technical environment, creating Disaster Recovery plans, and testing activities.

CHILI publish nv
Korte Keppestraat 9, Box 11
9320 Erembodegem - Belgium
info@chili-publish.com
+32 (0)2 888 65 11
VAT BE 0825.827.712

Business Continuity Recovery

Business continuity recovery point objectives (“RPO”) will be twenty-four (24) hours and recovery time objectives (“RTO”) will be twelve (12) hours or up to forty-eight hours (48) in case the disaster occurs between Friday 4PM and Monday 8AM CET, depending on support hours.

Recovery Point Objective (RPO) means, for a given function, the maximum tolerable period in hours in which data might be lost from such function due to a disaster or business continuity event.

Recovery Time Objective (RTO) means, for a given service, the duration of time in hours within which such service must be restored after a disaster recovery or business continuity event such that the Provider is providing the service and is able to meet the service levels associated with such service.

Non-Compliancy

The compliancy of the CHILI publisher software is affected when:

- The Subscription date is out of range
- The number of environments is not matching the subscription
- The amount of Renders and/or Storage is not matching the subscription
- Overdue invoice(s)

The effect of Non-compliancy is the temporary suspension of the CHILI publisher service for all environments and regions, until the compliance issue has been resolved.

Secure development (SDLC)

Framework Security Controls

CHILI publish leverages modern and secure open source frameworks with security controls to limit exposure to OWASP Top 10 security risks.

Quality Assurance

Our Quality Assurance (QA) department reviews and tests our code base.

Separate Environments

Testing and staging environments are logically separated from the Production environment. Service Data can only be used for testing (R&D and QA) in an anonymized way.

Vulnerabilities Management

Static Code Analysis

The source code repositories are scanned for security issues via our integrated static analysis tooling.

CHILI publish nv
Korte Keppestraat 9, Box 11
9320 Erembodegem - Belgium

info@chili-publish.com
+32 (0)2 888 65 11
VAT BE 0825.827.712

Vulnerability Scanning
CHILI leverages vulnerability management technology and tools to constantly guard against common vulnerabilities and exposures.

Third-party Penetration Testing
In addition to our extensive internal scanning and testing program, CHILI publish employs third-party security experts to perform detailed penetration tests on different applications within our family of products.

Authentication Security

Service Credential Storage
CHILI publish follows secure credential storage best practices by never storing passwords in human readable format, and only as the result of a secure, salted, one-way hash.

Additional product security features

Role-Based Access Controls
Access to data within CHILI publish applications is governed by role-based access control (RBAC) and can be configured to define granular access privileges.

Privacy certifications

Privacy Policy
See online or separate document for the privacy policy at CHILI publish

Security Awareness

Policies
CHILI publish is developing a comprehensive security policy covering a range of topics. This policy is shared with and made available to all employees and contractors with access to CHILI publish information assets.

Training
All employees and contractors attend a Security Awareness Training which is given upon hire and annually thereafter. All engineers receive annual Secure Code Training. The Security team provides additional security awareness updates via email, blog posts, and in presentations during internal events.

Employee vetting

Confidentiality Agreements
All new hires are required to sign Non-Disclosure and Confidentiality agreements.

CHILI publish nv
Korte Keppestraat 9, Box 11
9320 Erembodegem - Belgium

info@chili-publish.com
+32 (0)2 888 65 11
VAT BE 0825.827.712