# GDPR compliance and Data Security Policy at Netkin

*Last update: 17/08/2019*

This document describes how Netkin enforces GDPR compliance, and which measures are in place to ensure the security of the your data, as well as your participants personal data.

## What is GDPR ?

GDPR stands for “General Data Protection Regulations”, a new European-level regulation coming in effect on 25 May 2018.

The regulations are designed to **harmonize data privacy laws across Europe, enhance protection of EU citizens personal data, and improve the way organizations approach this data.** It’s very important to know about the changes, because non-compliance can mean heavy fines for businesses and organizations.

## As an event organizer, am I concerned ?

The biggest change is probably the extended jurisdiction of the GDPR. Starting 25 May 2018 the rules for data protection will apply to all companies processing personal data of EU citizens, regardless of the company’s location.

The GDPR will also apply to the processing of personal data for EU citizens, where the activities relate to: offering goods or services (free or paid) to EU citizens, as well as monitoring of behaviour within the EU. Non-EU businesses that process EU citizens data are required to appoint a representative in the EU.

**So yes, as long as some of your participants might be EU citizens, you are concerned, and your processes and tools must be GDPR-compliant.**

## What are the risks of non-compliance ?

If your business or organization is found to be in breach of GDPR you face a substantial fine. The maximum can be up to 4% of your annual global turnover or €20 Million, whichever is greater. The fines are imposed for infringements like:

- insufficient customer consent to process data;
- violations of the Privacy by Design concept;
- not having your records in order;
- failing to notify the relevant authority and data subjects about a breach.

# What are my obligations, what are Netkin obligations ?

GDPR defines two roles in the process of handling your participants data : Data Controller, and Data Processor.

## **Data Controller** (You as an event organizer)

Controller refers to the person or business that decides what pieces of information are collected, for what purposes, and in what ways it's being processed. According to EU law, the controller's obligations include, but are not limited to:

- provide clear information to your participants about the personal data you collect and for what purpose;
- obtain clear consent of the participant that he or she agrees to provide his/her personal data for this exact purpose
- provide the participant with an easy way to ask that you erase, cease further dissemination of the data, and potentially have third parties halt processing of the data, as well as restitute his/her personal data to the participant in a human readable format (excel for example)

**Netkin enforced since May 2018 that all registration website have a mandatory checkbox on the first registration step with a standardized text covering thoses 3 obligations. We strongly advise you to double check this text with your internal legal service, or the legal service of your client, to ensure it is compliant with country or company policies.**

Controller's obligations also include :

- hold and process only the data absolutely necessary for the completion of its duties (data minimisation). Additionally, they have to limit the data processors' access to that personal data.
- protect personal data against accidental loss, unauthorized access, or unlawful processing
    - **Netkin ensure this protection at the platform level (see bellow), but the security of your mailbox, computer, software, etc. are your responsibility**

- establish written agreements with processors that are given access to your customer's data, that require them to act only according to your instructions and make sure they comply with all data protection requirements.
- inform participants within 72 hours of first becoming aware of a data breach.
- ensure that all data processors fulfill requirements (see bellow)

## **Data Processors** (Netkin and our hosting company OVH, and your other subcontractors)

Processor is any person or business that processes personal data for the data controller, like registration platform, event app, data analytics, hosting or storage services, etc.

**IMPORTANT : If you export data from Netkin platform (for example as Excel file) you are a data processor as well, and obligations of Data Processors also apply to you and all your subcontractors that might have access to this exported data (freelance managing participant registration, or badge printing subcontractor for example).**

The requirements for processors include, but are not limited to:

- process data fairly, lawfully, and for legitimate purposes;
- implement all appropriate security measures to protect the personal data;
- informing the controller immediately of any data breaches.
- keep internal records of all data processing activities
- enforce privacy by design : this means the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically, you have to implement appropriate technical and organisational measures to meet the requirements of the new regulations and protect the rights of data subjects.

**Netkin implemented appropriate measures to be fully compliant with thoses requirements. (See bellow)**

# Data Security Policy at Netkin

## Privacy by Design

Since the beginning, **Netkin solution was built on the principle of Privacy By Design**

- Each event has its own platform (instance of our solution), running fully isolated on our dedicated servers hosted at OVH (we do not use public cloud), with its own private database

- Each event instance has no way to communicate with other event plaftorms, even on the same physical server
- Our automated deployment system cannot access event instances after deployment, only send them whitelisted configuration instructions
- Within an event instance, privileged users (administrators in charge of participant registration) are a fine-grained and fully audited access control
- All privileged user must by default authenticate using 2FA (autologin link with very strong hash + SMS confirmation code)
- Within an event instance, a participant cannot access other participant data, except in the participant directory, in which you can choose which fields to display. By default email, phone number, or other sensitive data are not included, in which case those data are not even downloaded on participant machines. Only privileged users that you (the main client administrator) appoint can access it
- Amongst Netkin project staff, no one can access the administration panel of your event platform without you granting explicit permission in your administration panel.
- Amongst Netkin technical staff, no one can access the source code or the data of your event platform without the approval of Netkin CTO or CEO.

## Automated pentests

- **Each of our release is scanned using Acunetix last version,** directly on production server, black-box and then white-box using AcuSensor Technology. This occurs nearly every month.
- **Upon request, we can perform a security scan of your instance** once it is ready, as anonymous user, and as logged in participant only (Security scan as privileged user will alter your platform content). This service occurs at a small fee, considered our low pricing.

## Human pentests

- Each new pre-release (usually monthly or bi-monthly) of our solution is pentested by Lexfo, ensuring no known security flaw goes to production. Last pentest result is available upon request.
- Several of our customers request to perform pentests or security scans of their own on a live instance. This can only be done within the following perimeter. By performing testing of any kind on one of our instance and/or server, you fully abide to the restrictions mentioned bellow. You might be responsible of any damage caused by not respecting those restrictions.
    - No technical access to the server will be provided (this is strictly non-negociable, as our source code is non-disclosed for security reason)

- Testing or scanning with privileged (administrative) account is strictly prohibited, since it can alter the website structure and/or content, and send unwanted emails. Privileged accounts have the ability to export all data anyway.
- No testing that might alter data and/or quality of service is allowed, since your target instance is on a production server
- No DDoS testing is allowed (our hoster OVH has datacenter level DDoS protection)
- Testing can only be done as anonymous user (not logged in) and regular participant (no privilege)
- You are not allowed to export or disclose any data you might have access to during the testing

## Staging and production servers security

- **Data is hosted exclusively in OVH dedicated servers in France**, located in OVH main datacentre in Roubaix (France), Gravelines (France), and Strasbourg (France)
  - Datacenter security measures : https://www.ovh.com/world/about-us/security.xml#datacentre
- **Front servers** (apache 2.4, php 5.x) : CloudLinux 7.x (Hardened version of CentOS 7.x), WHM/CPanel with CPHulk (brute force protection) and integrated firewalld. No client database on this server
  - Using CageFS technology (provided by CloudLinux), every instance runs in its own caged filesystem, and cannot see other instances files, data, processes, and cannot access sensitive files of the server configuration. More information on https://cloudlinux.com/index.php/cagefs.
  - None of our client has access to administrative or technical access to the server (no FTP or MariaDB access, no CPanel access, no shell access, etc.)
  - Fully automated updates and patches for CPanel and CentOS, with summary being sent by email to CSO, and human verification every month
  - ClamAV antivirus with automated daily scan
  - DDOS protection by OVH
  - Apache 2.4 / PHP 5.5
  - OWASP Apache ModSecurity CRS filter protection
  - CloudFlare WAF is available as an option
  - Administrative accesses to server are IP filtered at the firewall level (only our office IP address is allowed), and require technical approval of Netkin CTO or CEO.
  - Brute force protection is enforced on IMAP, SMTP and all services.
  - Logging: Server firewall, HTTP Daemon, CPHulk are producing access and error logs that are analysed every week against performance or security issues.
- **Database cluster servers** (mariadb 10.1.x) : CentOS 7.x, only port 3306 is allowed through the firewall, on private LAN (VRack by OVH), with on-disk encryption of data. This cluster is not reachable from the internet.

# Development security principles

**Each code contribution of our developers is reviewed by Netkin CTO/CSO**, to check for performance bottlenecks and ensure that every piece of code follows OWASP guidelines (https://www.owasp.org/index.php/OWASP_Code_Review_Guide_Table_of_Contents), amongst which :

- Development, test and prod envs are on physically separate networks (OVH v-rack) and physically separate servers
- Transport security:
    - https mandatory with fully trusted certificate, and HSTS
    - weak ciphers or protocols have been disabled
    - Qualys SSL Labs quality grade : A+
    - Report : https://www.ssllabs.com/ssltest/analyze.html?d=pentest.event.netkin.io&hideResults=on
- Password and authentication security : Authentication by password is forbidden by default, we use autologin links, which security is stronger since it does not involve a human element (the password). Besides, it avoids employees to put their corporate passwords by reflex. Autologin links work as follows:
    - Autologin links are using random token with very long verification hash : https://nameoftheventwebsite.com/trk/437-FDimZkGaIfmYdMDkimWT--nkwsid169-7a3505564affeec839987386ee0a41f0c08aeb2bb122b85d26e4d0a7fa4dde6e-c5d4156451-bfe7a71f3abc87ac28ecb051e2484b7c9dfa1ea917eb2921f69bda96f11b8c25
    - Unicity of every random string is enforced by storing their sha256 hash.
    - IP-based brute-force protection of 8 attempts, disabling the ability to authenticate for the IP during 30 minutes
    - Administrative access to the instance is reinforced by default using single-use two-factor authentification (Single use token link sent by email based on browser session, which has to be validated using single-use numerical code sent by SMS)
    - When a privileged user logs in from an unkown IP address, or from a new browser, all users with the user rights management privilege can be notified by email, with single-use link allowing immediate account locking
    - Authentication cookies and session cookies are HttpOnly and Secure. Our application stores a hashed representation of the cookie's value when it gets sent, and then compares the received cookie's value to ensure they are the same.
- Mixed Content :
    - All ressources are loaded from domain name, no use of CDN

    - Cross Site Request Forgery (XSRF or CSRF) : Requests triggering data modification are only done through POST. Each POST request is validated with CSRF token. If missing or wrong, the request is blocked.
    - Cross Site Script Inclusion (XSSI) : All JSON requests are done through POST only
    - Clickjacking : header  X-Frame-Options: SAMEORIGIN sent on each page
- 3rd Party Content : all ressources are served from website server and domain name
- Input Validation
    - SQL Injection : All requests containing user input use parametized queries
    - XPath Injection : no use of X-Path
    - LDAP Injection : no use of LDAP queries
    - Command Injection : no use of command line in php code
- Path Traversal : image autosizing and croping validates MIME type of the file being requested, and is limited to user content images directory
- Cross Site Scripting (XSS) : Data collected from user is stored, and displayed, using appropriate escaping function
- Integer Overflows : for each numerical input, length and type are validated
- XML External Entities : No XML ressources loaded from outside system

## Netkin office security

- Local network protected by WatchGuard Firebox M200 appliance
- Avast Business Antivirus (Fully functional payed version, with centralized management system and auto-update, high heuristic sensitivity with code emulation, and integrated firewall. Users cannot desactivate, uninstall or configure the antivirus.)
- Intrusion detection and fire detection by Securitas Direct / Verisure (certification APSAD R31 P3)
- CCTV of all access to our office, with 30 days retention.
- Email accounts of our employees are Gmail Enterprise accounts with 2FA enabled
- No wifi access allowed to local network

## General staff security policy

- All employees are full-time, CDI, and have signed specific NDA covering all internal and client data.
- No part-time or external workers have access to client instances, unless explicitly authorized by the client.
- Only required employees are allowed to access data, and are not allowed to keep a copy of data. All employees have signed this as part of their NDA

- Employees are not allowed to keep copy of client data outside of the client instance. All provisory copy (received by any bias, including email, or extracted from the client instance must be deleted immediately after use). All data extraction shall be done by the client using his/her administrative access to the platform, we do not accept to perform data extraction on behalf of our clients.

# Technical staff security policy

- Development on local server in our offices, testing and staging server at OVH, with automated antivirus scan, automated and human functional testing, and Acunetix OWASP scan performed by CSO on each release candidate.
- Production instances are then deployed automatically by a home-made deployment application located on a dedicated server, access to which is IP filtered. This solution install source code, database, mailboxes, SSL certificates, and sends administrative access to the client, which is then able to grant access to our project team if necessary.
- Developers do not have access to the staging application source code, database or server.
- This ensures that our employees do not have access to clients production instances, unless explicitly allowed by direction or client (only upon written email request, no phone request allowed).

# Business continuity policy

Every instance is backuped once a day on a secure off-site OVH datacenter. Backups are retained daily for one week, and then weekly or monthly, until data destruction (see bellow).

- Daily automated database and user files backup, crypted with AES-256-CBC, to secured storage server. **RPO** is thereby of 24 hours.
- Monitoring of automated backup
- Data recovery and business continuity in case of server failure (**RTO**) :
    - **Registration website (used before the event) :** 4 hours
    - **Event live application (user during the event, amongst others for interactivity sessions)** : Load balancing is performed at the client level with the following principle : each client looks for the fastest responding server amongst 4, which are located in 2 distinct datacenters (Roubaix in France, and Strasbourg in France). Each server contains the same replica of data, and is synced realtime with the others, with full network failure tolerance and recovery. With the architecture, even in the very unlikely event of failure of 3 servers at the same time, the app will still be fully operational.

We commit to a 99,95% SLA on platform general availability. This exclude any misconfiguration made by the client when self-administering the platform, as well as misconfigured or obsolete clients that might not be able to access or display the registration website or event app.

## Data conservation policy

By default we keep the data of an event instance for one year after deployment. Data is then automatically erased, including backups.

If needed, you can ask us to increase or reduce this period.

## Any question ?

If you need additional information, you can contact us at support@netkin.fr