DataEngine B.V. information security policy

Version: 20180426

Introduction

DataEngine B.V. places privacy, security and transparency at the top of its list of priorities. We believe it is important to inform our customers properly about the measures we take to protect (personal) data. On the one hand, we do this to give you a feeling of peace of mind but, at the same time, this provides you with tools to make the right assessment as to whether these measures are sufficient for the type of data you want us to process.

General organisational measures

Within our company there are a number of measures that we take to protect data against loss, theft or illegal use. Below are the measures we have taken on an organisational level.

1. Our employees only have access to the data they need for the performance of their job.
2. In order to gain access to data, we have applied multiple (independent) layers of security. A number of examples of measures are: multi-factor authentication, the use of VPN to encrypt network traffic and the application of IP Access Control Lists, firewalling and the use of strong passwords.
3. Personal data may never be stored in our company in other places than agreed upon. We have internal procedures for this. If applicable, this also includes a retention policy to remove (copies of) personal data after use.
4. We have a confidentiality agreement with our employees.
5. We have an internal Security Awareness programme for our employees.
6. We work with a rating system for code. New functionalities or modifications to current systems go through a fixed review and roll-out process.
7. We use a password management system. This allows us to impose and monitor a security policy on our employees regarding the use of password-based accounts.
8. Employees have their own laptop. This equipment is never shared with anyone else. The data storage on these systems is encrypted.
9. We ensure that employees who leave our company no longer have access to data.

10.

Technical measures against unauthorised access to data

In addition to organisational measures, we also take technical measures. Some of these are a fixed part of our services and cannot be switched on or off as a customer. We offer a number of other measures, that may not activated by default.

1. Our systems are equipped with a firewall. Only IP traffic that is explicitly allowed can exchange network traffic with our systems
2. Two factor authentication is enabled for access to services.
3. We use strong and modern hashing algorithms to store passwords.
4. In order to detect and automatically block brute-force attacks, we use an intrusion detection system.
5. All the services we offer have an SSL certificate with strong and modern network encryption.
6. We keep track of what the cryptographic standards are and update our encryption algorithms when needed.
7. We will ensure that the software we use to provide our services is up to date.
8. We apply segmentation between systems as much as possible. For this we use containerisation, virtualisation and in other cases physically separate hardware. We use this segmentation to provide systems with as many layers of security as possible with a different risk profile, function and scope.
9. Network communication of the systems under our control always takes place via an encrypted connection.

Measures to ensure business continuity and data accuracy

1. We periodically check the integrity of the data stored with us.
2. We check the integrity of the data 'in-transit' and after it has been written to fixed storage and encrypted.
3. We only use enterprise-grade hardware. Some examples of this are the use of Error Correction Code (ECC) memory and SAS drives.
4. We have in-depth monitoring of our platform and systems.
5. In the event of disruptions to our services, personnel are available 24 hours a day, 7 days a week to rectify these disruptions as quickly as possible.
6. We are independent of a network provider and manage our own connections to and from the Internet.
7. We use a separate development, testing and production environment.
8. We make periodic backups, check their integrity and store them in a geographically separate location in encrypted form. A retention policy has been applied to these backups.
9. We equip used hardware redundantly.

Information about the data centres we use

We only install our servers and other equipment in the most modern data centres. These data centres offer us the right security against burglary, fire, power failure and other calamities. These data centres have taken the following measures to meet these requirements.

1. There are strict login procedures to gain access:
   • Only persons who are on the predefined access list have access.
   • Upon arrival, your identity will be checked by qualified security personnel and a biometric scan. Strict registration procedures apply to working visits.
2. The data centres are accessible 24 hours a day for our employees..
3. Our equipment is installed in locked racks.
4. We only use Dutch data centres.
5. There is permanent camera surveillance.

6. Power supply is guaranteed by the use of UPS systems and emergency power units. For long-term disruptions in the electricity network, supply agreements are in place for replenishing the fuel for the emergency generators.

7. We use separate feeds for the supply of electricity to our equipment. Each feed in turn has its own UPS system.

8. The electricity feeds we use have more than sufficient overcapacity.

9. Equipment is placed on elevated data floors.

10. The data centres have redundantly equipped climate control.

11. There are sufficient measures in place to prevent or delay physical break-ins to these locations. A number of examples are: secure fencing, tombstones and extra thick walls.

12. These data centres are equipped with advanced fire detection and extinguishing systems.

13. These data centres comply with all current certifications (available on request from your contact person).