TRANSPARENCY STATEMENT REGARDING PROCESSING PERSONAL DATA

KE-works B.V. | version 1.0 | April, 2018

1 INTRODUCTION

KE-works is a company (a private limited liability company) located in in Delft, registered at the Chamber of Commerce under number 50797832. This company provides its clients the KE-chain platform, a cloud based app platform, which enables its clients to develop applications for digital engineering and operations.

This transparency statement is intended to inform clients and users about how KE-works:

- handles personal data;
- has taken measures in order to prevent unlawful processing of personal data.

2 WHO

Who are the actors?

The applicable privacy legislation makes a distinction between several actors. The most important ones are: controller and processor. In this case the controller is the client of KE-works, since the client determines the purpose(s) for which the personal data is processed, and with which means this will happen. KE-works is processor. On behalf of its clients, it processes personal data. Data subjects are the users, administrators and/or developers.

To provide the services, KE-works uses Amazon AWS, Digital Ocean and Leaseweb. Therefore, they are deemed sub-processor.

3 WHAT and WHY

What is being processed? And why is the data processed?

Hereunder is explained which categories of personal data are processed, which kind of personal data is involved, and for what purpose(s) these personal data is processed. In the infrastructure of the KE-chain platform there is a distinction between “core” which is solely developed by KE-works and “client application” which is designed and developed solely and independently by client. With the KE-chain platform a client application can be developed on top of the core. KE-works does not know what sort of (personal) data a client process outside the core of the Software. This is why it is the responsibility of client to implement adequate business rules and/or take technical and organizational measures to secure the personal data processed outside of the core of the Software.

Category	Personal data	Purpose
Core	Name	Identifying user
	Password	Login user
	E-mail address user	Login user
Client application	Client uses the KE-chain platform to create its own apps and/or functionality. Which means that a client of KE-works may be able to process more personal data than mentioned above.	Determined by client

4 WHERE?

Where is the personal data processed?

KE-works guarantees that the personal data will only be processed within the E.U. / E.E.A.

5 UNTILL WHEN DATA WILL BE PROCESSED?

What are the retention periods for the different categories of personal data?

Below is explained how long personal data are stored.

Category	Retention period
Core	For the duration of the agreement entered into between KE-works and client, or so much sooner in case clients deletes a user. Client should be aware of the fact that after deletion data is available for one month in the back-up. This back-up should be take into account by deciding the retention period.
Client application	For the duration of the agreement entered into between KE-works and client, or so much sooner in case of (automated) deletes by client. Client should be aware of the fact that after deletion data is available for one month in the back-up. This back-up should be take into account by deciding the retention period.

6 HOW?

Which kind of technical and organizational measures have been taken to protect the personal data against unlawful processing?

The list below sets out which measures are taken by KE-works to protect the processing of personal data against unlawful processing. This list is not exhaustive.

Category	Measures
Personnel	• A confidentiality clause has been incorporated in the employment agreements and agreed with employees of KE-works. This confidentiality obligation also covers personal data of clients. • KE-works staff have access to the equipment and / or software with which the personal data of the client are processed on a need-to-know basis.
Organizational	• Personnel are trained in privacy awareness. • KE-works periodically evaluates the impact of its services on the privacy of those who are involved (employees or clients). KE-works records the outcome.
Technical	• Personal data in transit are always encrypted with a valid SSL certificate. • Passwords one way encrypted. • In further developing the software that underpins the service, KE-works endeavors to comply as much as possible with common practice security standards.

7 DATA SUBJECTS

Exercising rights by data subjects.

The privacy legislation offers data subjects, the possibility to invoke their rights to which they are entitled according the law. This concerns, for example: right to information, right to access and right to rectification, right to erasure ('to be forgotten') and right to object, right to restriction, right to data portability, right not to be subject to automated individual decision-making.

KE-works always forwards the requests to its client. It will not handle the requests itself. After forwarding KE-works will inform data subject about the forward. The client of KE-works must then handle the request, possibly supported by KE-works in case desired, by the client.

8 COOKIES

Does KE-works uses cookies?

Our cloud-based platform KE-chain uses cookies. A cookie is a small text file which is send with every page request to our webserver. The text file is saved by the browser on the hard drive and/or storage of the computer or device of the user. At the next visit the information stored therein can be sent back to our servers.

For functional cookies (see below) and for cookies from Google Analytics (see below) KE-works does not request permission. For all other cookies KE-works requests permission to store cookies.

The cloud-based platform KE-chain uses session cookies. These session cookies are standard used by the programming language with which the application is programmed. These session cookies mainly provide an easy and undisturbed use of the website. The session cookies are automatically removed from the device when the browser is closed. If the application contains functionality to log in, the website can use a (session) cookie to detect whether the user is logged in.

By using the cloud-based platform KE-chain Google Analytics, Google will set cookies through our website. KE-works uses Google Analytics to keep track of, and report regarding the usage of our website by users and visitors. Google may disclose this data to third parties in case it is obliged to do so by virtue of law or court order, or in case third parties process data on behalf of Google. We entered into a data processing agreement with Google. By doing so, Google is not allowed to use the collected information for other purposes and/or other Google services. Furthermore, we configured Google Analytics in a way that IP addresses will not be forwarded to Google.

9 GENERAL DATA PROTECTION REGULATION

To which extent is KE-works and its services GDPR compliant?

The GDPR, General Data Protection Regulation, will replace the Data Protection Directive 95/46/EC. When it comes to the question of the extent to which KE-works and its services are GDPR compliant, this is mainly a combination of how the client of KE-works meets the GDPR and which measures KE-works has taken. In the sheet below is an overview of the most important points from the GDPR with who is responsible for compliancy. This list is not exhaustive.

#	Requirement from GDPR	KE-works	Client
1	For processing personal data there must be always a lawful basis.	☑ KE-works processes the personal data on behalf of the client in order to provide the agreed services.	☐ The client must determine a valid lawful basis for processing the personal data.
2	Prohibition to process special categories of personal data.	☑In principle, KE works does not process special personal data.	☐ It is the responsibility of client to ensure that it will not ask questions or data from users, which will lead to collecting special personal data.
3	Prohibition processing legal identification numbers. (for example Citizen Service Numbers (BSN))	☑ In principle, KE works does not process legal identification numbers.	☐ It is the responsibility of client to ensure that it will not ask questions or data from users, which will lead to collecting legal identification numbers.

5	Appropriate technical and organizational measures must be taken in order to guarantee the required level of protection.	☑See paragraph 6 of this transparency declaration.	☐ The client must also take technical and organizational measures.
6	Where necessary, anonymization, pseudonymizing or encryption must be used.	☑KE works encrypts passwords. And aggregates and anonymizes data.	☑
7	When outsourcing activities where personal data are involved, there must a data processing agreement.	☑With the subcontractors who are processing personal data KE-works has entered into a data processing agreement.	☐ The client of KE-works can optionally accept the new general terms and conditions of KE-works in which a basic data processing agreement is included, or - if the client demands a separate processor agreement - the client can be provide with a standard data processing agreement.
7	After processing, the personal data must be deleted or returned to the controller and then deleted, this at the discretion of the controller.	☑The KE-chain platform enables client to liberate its data. For example with an API or export functionality. After the agreement is terminated, KE-works deletes all data.	☑
8	For enabling and using sub-processors a general or specific consent is required.	☑For enabling and using sub-processors KE-works has obtained general consent from the client through accepting the general terms and conditions or the agreeing separate data processing agreement. However, KE-works will notify timely when new sub-processors will be involved.	☐ The client of KE-works can optionally accept the new general terms and conditions of KE-works in which a basic data processing agreement is included, or - if the client demands a separate processor agreement - the client can be provide with a standard data processing agreement.
9	Prohibition of processing or transferring personal data outside E.U. / E.E.R. unless the country has an adequate level of protection.	☑See section 4.	☑
10	In some cases, a Data Protection Impact Assessment (PIA) is a mandatory obligation.	☑Although KE-works is not obliged, KE-works carries out annually an PIA. Upon first request of client, KE-works is willing to cooperate.	☐ Client must investigate independently whether it should carry out a Data Protection Impact Assessment (PIA).
11	Internal registration of processing.	☑KE-works records which personal data of clients she stores and process. Also KE-works has the client's contact in case of security incidents has occurred during the processing.	☐ Regardless KE-works records the processing, the client must record with its own management tools the processing of personal data by using the services of KE-works.
12	In some cases, the appointment of a Data Protection Officer is mandatory obligation.	☑KE-works is not obliged to appoint a Data Protection Officer. KE-works has therefore not appointed a data protection officer.	☐ The client must check for itself and consider whether it appoints a Data Protection Officer with regard to the processing of personal data.
13	Reporting security incidents or data breaches.	☑KE-works reports security incidents or data breaches to client as soon as possible. This is also stipulated in the general terms and conditions and the separate data processing agreement.	☐ It is the responsibility of client to ensure that it has an adequate procedure to find out whether the incident of data breach KE-works has reported is a data breach as referred to in the GDPR, and whether a notification to the supervisory authority is required and should be done.

10 AMENDMENTS

KE-works reserves the right to change this transparency statement at any time. Therefore, consult this statement regularly to make sure that you are familiar with the latest version.