ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

Report AVG/GDPR-scan

abn amro rotterdam: 24.00.46.420
iban: NL13 ABNA 0240046420
swift-adres: ABNA NL2 A

handelsregister rotterdam
nummer 24159043

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

Table of contents

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

1. Objective

This scan is executed with the objective of mapping data processing within the framework of the new AVG legislation. And to make recommendations based on the findings to be compliant with the AVG legislation.

Conversation with:
John Vrij (Head of Administration)

1.1 Rated components

• Procedures regarding the protection of personal data within KE Holding B.V., KE Expeditie B.V. and KE France B.V. **(hereinafter "KE")**

• Data flows regarding the new legislation for the protection of personal data.

• Protection of the systems and data regarding the processing of personal data.

• Permission structure within KE regarding the processing of personal data.

• Knowledge within the organization regarding the protection of personal data.

• Compliancy

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

2. Policy document for information security

The policy document explicitly discusses the measure that the Processor takes to protect the Processed Personal Data. The document has been approved at administrative or managerial level and made known to all employees and relevant external parties.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

3. Data flows related to Personal data

3.1 Job applications

How do application documents arrive at KE?
The applications arrive in a designated mailbox with an email address that is stated on the website of KE.

What information is stored of applicants?
- Name and surname
- Address data
- Telephone number
- Email address
- Date of Birth
- Curriculum Vitae
- Experience
- Education
- Passport photograph
- Copy of identity document

Everything that an applicant wishes to share in his or her CV and application.

Where and how are the data of the applicants stored?
If successful, these documents are digitally stored in a designated mailbox and physically stored in the
designated lockable closet in the office to which only authorized persons have access.
In the event that an application has not been successful, this data will be deleted immediately.

Who has access to this information?
These documents are accessible to the management, head of administration and the secretary of KE.

How is this data protected against a data breach?
- This information is only accessible to authorized persons within KE.
- This data is protected in accordance with the information security policy of KE.
- This data is protected according to the Microsoft Office information security policy.

How long is this information stored?
- This information is kept as long as the employee is employed by KE.
- This information can be removed on request within four weeks after the application procedure.
- Upon request, this information can be deleted within four weeks of the employment.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

3.2 Salary processing

How is the financial administration being done?
The financial administration is done with the web-based application of BCS HRM & Salary administration B.V.

Which personal data is kept in the financial administration?
- Name and surname
- Address data
- Annual statements
- Salary specifications
- Bonuses
- Bank information
- BSN number
- Holidays
- Absence
- Declarations

Where and how is this data stored?
This data is processed in the web-based application of BCS HRM & Payroll.

Who has access to this information?
This information is accessible to the authorized persons within KE and for the relevant persons whose data is through a personal account.

How is this information protected?
- This data is stored encrypted in the online platform of BCS HRM & Payroll.
- This data is protected in accordance with the information security policy of BCS HRM & Payroll.
- This data is not used for purposes other than those for which explicit permission has been given.
- This information is only accessible to authorized persons within KE.
- This data is protected in accordance with the information security policy of KE.

How long is this information kept?
This information is retained for the period prescribed by Dutch tax legislation.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

3.3 Personnel files

How are the personnel files kept up to date?
The personnel files are recorded and kept up to date both physically and digitally.

Which employee data is recorded and saved in the personnel files?
- Absence
- Training followed
- CV
- Application Documents
- Summaries of assessment interviews
- Official warnings

Where and how are these files stored?
These files exist in both physical and digital form. The physical items are kept in a lockable closet intended
for this purpose. The digital version is in a designated folder on the server systems of KE.
Who has access to this information?
This information is accessible to the management of KE and for the head of administration.
This information is also available on request for the persons in question whose data it belongs to.

How is this information protected?
- This information is only accessible to authorized persons within KE through the use of a personal account and password.
- This data is protected in accordance with the information security policy of KE.
- This data is stored in a designated folder on the server systems of KE.
- This data is physically stored in a lockable closet intended for that purpose.

How long is this information stored?
This information is kept as long as the employee is employed by KE. After an employee leaves the company, this information can be removed within four weeks upon request.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

4. Responsibilities for information security

All responsibilities with regard to the protection of information, both at management and executive level, must be clearly defined and established.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

5. Security awareness

All employees of the organization and, where applicable, hired staff and external users receive appropriate training and regular training on the organization's information security policies and procedures, as relevant to their position. Within the training and retraining, explicit attention is directed to the handling of (special or otherwise sensitive) personal data.

At KE there are no staff meetings about legislation and regulations, explicit attention must be directed to the handling of personal data. Procedures must be established for reporting data breaches. No procedures have yet been established for dealing with a security incident.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

6. Physical protection and protection of equipment

IT facilities and equipment are physically protected against unauthorized access and against damage and disruptions. The protection offered is consistent with the identified risks.

The network equipment of KE is located in a physically enclosed space and is equipped with appropriate security. All critical business applications are Cloud-based or are managed by third parties with which there must be a clear processing agreement that guarantee AVG compliance.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

7. Security access

There are procedures to give authorized users access to the information systems and services they need to perform their duties and to prevent unauthorized access to information systems. The procedures cover all stages in the lifecycle of user access, from the initial registration of new users to the final logout of users who no longer need access to information systems and services. Where applicable, special attention is directed to managing access rights of users with extra broad powers, such as system administrators.

Users can only log in with their own personal password. The user only has access to the personal data that applies to their person or project. All other personal data is secured and not accessible. The system uses a permission structure at main and sub level. When a user leaves service, access to the systems and services of KE will be denied.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

8. Logging and checking

Activities that users perform with personal data are recorded in log files. The same applies to other relevant events, such as attempts to gain unauthorized access to personal data and disruptions that can lead to damaged and or loss of personal data. The log files are periodically checked for indications of unauthorized access or use of the personal data and action is taken where necessary. The processor must take into account that, if the data in the log files are traceable to persons, there is a processing of personal data in the sense of the applicable privacy legislation. In that case, there may also be a personnel tracking system within the meaning of Article 27, paragraph 1, of the Wet op de Ondernemingsraden (WOR) (legislation for work councils), for which the approval of the work council is required.

A computer logging system called Activity Monitor is used. All staff are aware of this and have given written permission for this. The log files are kept indefinitely and can be deleted on request within four weeks. The systems of KE does not draw conclusions from the collected data. This data is used to optimize own business operations and to prevent unauthorized use of systems from KE track down. Under no circumstances is this data shared with third parties or used for other purposes only when explicit permission has been given.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

9.Processing in application systems

Security measures are built into all application systems, including applications developed by users themselves. These security measures include checking that the input, internal processing and export meet predefined requirements (validation). Systems that process special or sensitive personal data or that affect the processing of special or sensitive personal data may require additional security measures.

Every user logs in with a personal account, this account has a specific role within the system with only access to the data that the person needs to perform their work. All operations are logged, the logs are periodically checked by the designated people within KE.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

10.Management of technical vulnerabilities

Software, such as browsers, virus scanners and operating systems, are being kept up-to-date. The processor also installs the most recent updates that the supplier of the relevant software releases for security breaches in this software. More generally, the controller obtains the most recent information about technical vulnerabilities of the information systems used. The extent to which the organization is exposed to such vulnerabilities is evaluated and the processor takes appropriate measures to deal with the associated risks.

The workplaces and the network of KE are periodically updated. Virus scanners and firewall software on the computers perform an update round every day. This guarantees that all computers within the organization are protected against the latest vulnerabilities. The server systems of KE are also appropriately secured and periodically perform updates on both operating system and antivirus software. The server systems of KE perform regular backups, these are also checked weekly by the system administrators of KE.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

11. Incident administration

There are procedures for the appropriate and effective handling of information security incidents and security vulnerabilities as soon as they are reported. The assessing of risks for those involved and effectively informing those involved and, where applicable, the supervisor are included in these procedures. The information learned from the handled incidents are used to structurally improve security where possible. If a follow-up procedure following an information security incident includes legal measures (civil or criminal), the evidence is collected, stored and presented in accordance with the rules for evidence established for the relevant jurisdiction.

There have to be procedures and be carried out if required. Monitoring takes place at the workplace, system security, application security and access to personal data. If suspicious activities take place, immediate action is taken. Then the problem is analysed and a solution is provided so that it no longer occurs.

abn amro rotterdam: 24.00.46.420
iban: NL13 ABNA 0240046420
swift-adres: ABNA NL2 A

handelsregister rotterdam
nummer 24159043

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

12. Processing of data breaches and security incidents

The processor must report data breaches that are subject to a legal obligation to report in accordance with the procedure with the Dutch Data Protection Authority. These procedures have not yet been established at KE.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

13. Continuity administration

Personal data may be lost due to natural disasters, accidents, equipment failures or intentional acts. By setting up continuity management within the organization, the consequences are limited to an acceptable level, whereby a combination of preventive measures and recovery measures is used.

The storage and processing of personal-sensitive information is partly done in Cloud-based platforms, which guarantees that no information will be lost if a calamity occurs on location. The data is partly on the server systems of KE who regularly makes a backup so that if a disk fails, there is still no critical data loss.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

14. Authorization matrix

	Personnel files	Absence/sickness notifications	Financial administration	Customer files	Application documents
Management					
Head of Administration	v	v	v	v	v
Assistant administration	v	v	v	v	v
Operational Employees					
Accountant			v		
Secretary					v

abn amro rotterdam: 24.00.46.420
iban: NL13 ABNA 0240046420
swift-adres: ABNA NL2 A

handelsregister rotterdam
nummer 24159043

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

15. Website

It is a legal requirement to clearly inform your customers and visitors about which privacy-sensitive data you collect and for what purpose. Even if that goal is just to record their data in your customer base. This follows from the Personal Data Protection Act. Information is usually done via a privacy statement, also known as a privacy statement. Visitors must be able to find these easily. For example, place a hyperlink to the privacy statement at the bottom of every page if you collect statistical information about visitors, and refer to the privacy statement in the ordering process. The website offers the possibility to send a contact request email. The website is not secured with an SSL certificate. The website can be visited with the following link: http://ke.nl/. On the website of KE no privacy statement has been placed yet. Cookies are used that are not mentioned when visiting the website.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

16. Conclusions and recommendations

16.1 Conclusions

• The premises where KE is located are suitably secured through electronic door locking and access via intercom.

• The spaces where network equipment and data-carrying equipment are located are locked to unauthorized persons.

• Sensitive personal data cannot be viewed or processed by persons who are not authorized to do so.

• Sensitive or otherwise personal data is not shared with third parties for commercial purposes. Or used for purposes other than those for which explicit permission has been given.

• Connection to the network of KE is only possible with a secure VPN connection.

• There are clearly defined profiles, permissions and roles within the organization.

• The work processes are designed in such a way that protecting sensitive personal information has priority.

• There is sufficient knowledge on this subject with both operational staff and management.

• The server systems of KE are suitably secured and only accessible to authorized persons or parties within or outside the organization.

ke expeditie b.v.
parklaan 30 / 3016 bc rotterdam
t. 010 4 366 466 / f. 010 4 362 502
info@ke.nl / www.ke.nl

16.2 Action points

• The parties to which KE communicates sensitive personal information have received a processing agreement or have received the request from KE expedition B.V. to prepare a processor agreement.

• The withdrawal procedures must be clearly established and complied with in accordance with the AVG /GDPR.

• A clear division of roles will have to be established that dictates who is responsible within the organization for protecting / securing personal data. Should the situation of a data breach or security incident occur, this person will also ensure that this is assessed and will report this through the correct procedures and channels.

• Procedures must be established for dealing with a data breach or security incident.

• An information security document must be created.

• A processing register must be created.

• A privacy statement must be placed on the website.

• A processing agreement must be placed on the site or a link to a processing agreement.

• A processing agreement must be signed by the staff.

• Cookie use must be stated clearly.

• A SSL certificate must be added to the website to guarantee a secure connection.

• Personnel within the organization could follow a training or information day on how to deal with personal data if this applies to their work or powers within the organization.

• The mailboxes where personal-sensitive information is received and stored must be archived in time and in accordance with the AVG / GDPR.