Networkapp
Privacy Policy

Outline

Personal Data Protection

Networkapp

Networkapp offers an online platform and mobile application that enables people to connect and share knowledge. For our clients we offer a tool that simplifies the registration process, offering information within a community platform and event management.

Privacy policy

Privacy mission

Our customers and their relations, users, our employees and the organisations we work with must be able to trust that only the necessary personal data are processed, that this is done in accordance with the law and in a careful, transparent and respectful manner and that this contributes to the feeling of trust and safety for everyone involved.

Incidents in the area of privacy and with regard to the processing of personal data may in the first instance without serious measures have serious adverse consequences for the privacy of our customers, end users and/or employees, but in the second instance may also lead to serious consequences for our organisation itself. For these reasons, our organisation sees it not only as a duty but also as a social responsibility to take appropriate measures to prevent incidents, or to limit the risks to a minimum, to communicate about this openly and transparently and also to periodically judge/have it judged.

Legal framework

Our privacy policy obliges our organisation to comply with the legal principles relating to the processing and protection of personal data. The starting point for our privacy policy is formed by the following laws and regulations: AVG, UAVG, Telecommunications Act (including cookie legislation).

Our policy relates to the processing of data of all parties involved: Customers and their relations, users of the Networkapp, employees and third parties to whom services are provided or with whom cooperation takes place.

Since both legislation and technology are undergoing rapid development and our own organisation is dynamic and subject to change, it is necessary that the privacy policy is evaluated annually and adjusted where necessary.

Definitions

Autority Personal Data (AP): the supervisory authority, the independent body that ensures that personal data are processed carefully and safely and, if necessary, can impose sanctions if this is not done.

Person concerned: the person to whom a personal data relates, usually the user of the Networkapp, the customer and other relations and the employee.

Special personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and genetic data, biometric data for the unique identification of a person, or data on health, or data related to a person's sexual behaviour or sexual orientation.

Third party: any person or body that is not a data subject, controller, processor, or person authorised to process personal data under the direct authority of the controller or processor.

Data protection officer (DPO): official appointed for informing, advising on and supervising the application and compliance with the GDPR and other data protection provisions.

Infringement related to personal data: a breach of security that inadvertently or unlawfully leads to the destruction, loss, modification or unauthorised disclosure of or unauthorised access to transmitted, stored or otherwise processed data. A 'data breach' therefore includes not only the release (leakage) of data, but also unlawful processing of data.

Personal data: any information about an identified or identifiable natural person ("the data subject"); an identifiable natural person who can be identified directly or indirectly, in particular by means of an identifier such as a name, an identification number, location data, an online identifier or one or more elements characteristic of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

Pseudonymisation: the processing of personal data in such a way that the personal data can no longer be linked to specific data subjects without the use of additional data, provided that these additional data are stored separately and technical and organisational measures are taken to ensure that the personal data are not transferred to an identified or an identifiable natural person.

Approval of the person concerned: permission given by the person concerned, specific, freely and unambiguously and on the basis of good information, in which the person concerned accepts him regarding the processing of personal data. This can be done by means of a written or oral statement or an unambiguous active action (such as electronically checking a box). In the event that processing of special personal data cannot take place on a basis other than consent (e.g. legal obligation or agreement), there must be *explicit* consent, characterised by an explicit *expression* of will.

Processor: the person who processes personal data on behalf of and for us (as controller) (for example an external hosting company, SaaS supplier, quality auditor or an external payroll administration office).

Processing of personal data: all actions relating to personal data, including in any case collecting, recording, organizing, storing, updating, modifying, retrieving, consulting, using, providing by means of forwarding, dissemination or making available in another form, bringing them together, connection, and the protection, erasure or destruction of data.

Controller: the person who, alone or together with others, determines the purpose of and the means for the processing of personal data; usually the management of the organisation.

Obligations for our organisation

In addition to assigning rights to individuals whose personal data are processed, the GDPR contains a number of obligations for organisations that, in the context of their business operations, process personal data. The AVG applies to the way in which personal data is processed within our organisation. In this context, the principles used by the AVG are leading. In concrete terms, this means that every processing of personal data complies with the following principles:

- the processing is lawful, proper and transparent;
- the processing is tied to specific goals;
- the personal data are adequate, relevant and limited to what is necessary;
- the data is correct;
- the data is not saved longer than necessary;
- the data is secure and confidential.

Our entire organisation is responsible for compliance with the above principles. The mere taking of measures to ensure that processing of personal data takes place in accordance with the AVG is no longer sufficient. Networkapp as controller must also be able to demonstrate this and have proof of this.

In the context of the accountability arising from the GDPR, the following measures are taken, which show that the processing of personal data takes place in accordance with the principles of the GDPR:

A. Register of processing activities

To demonstrate compliance with GDPR obligations, Networkapp keeps a written record of the processing activities for which it is the controller. The register is a summary of the most important information about all processing of personal data that take place at Networkapp. If a particular processing activity changes, the registry is modified accordingly.

The register must be made available to the AP whenever it so requests. The FG of Networkapp also has access.

B. Data protection officer (DPO)

The AVG assigns an important role to the data protection officer (DPO). The DPO supervises and advises internally on the application and compliance with the GDPR by Networkapp. Based on GDPR's criterion of large-scale processing of special personal data, Networkapp is obliged to appoint a DPO. The function of DPO is fulfilled at Networkapp by an expert person.

C. Risk analysis: data protection impact assessment (DPIA)

If an intended processing of personal data is likely to pose a high risk to the rights and freedoms of natural persons, Networkapp implements a DPIA prior to processing. This is an assessment of the effects of a proposed processing activity on the protection of personal data and the rights and freedoms of data subjects. On this basis, measures are taken to prevent or reduce these effects for those involved.

Performing a DPIA is an integral part of the change management process implemented at Networkapp. With each organisational, hardware and/or software change to be implemented, it is determined whether personal data are involved and, if so, whether there is probably a high risk for the privacy of the data subject.

D. Privacy by design and privacy by default[1]

This principle is a concrete duty flowing from the GDPR for Networkapp. The principles of Privacy by Design and Privacy by Default are included by Networkapp as data protection requirements in the development of new policies or the design or purchase of new systems with which personal data are processed. This also applies to redeveloping existing policies and redesigning existing systems. Networkapp ensures that the new or renewed processing activities minimise the personal privacy of the data subject.

Networkapp can demonstrate that in the development of new policy or the design or purchase of new systems or the development of new work processes, it has ensured that the infringement of the protection of personal data for those involved is minimised by taking internal policy measures and by applying technical measures.

E. Information security

Security is an essential part of the privacy policy for Networkapp. Responsible handling of personal data falls or stands with adequate data security. Networkapp has taken a large number of technical and organisational measures to secure the personal data. By conducting risk analyses, it is determined whether the measures are appropriate, that is, tailored to the risk.

F. Data leaks: infringement related to personal data

Under certain circumstances, Networkapp is obliged to communicate a personal data breach, better known as a data leak, to the AP and the data subject. Given the major consequences that a data breach can have for the data subject, it is important that Networkapp tackles a data breach in a timely and appropriate manner. The compulsory notification to the AP and, where appropriate, to the person concerned is an elaboration of this.

G. Processor's Agreement

When an external party meets all of the criteria below, it is considered by Networkapp to be a processor:

- The external party is not subject to the direct authority of Networkapp.
- The external party acts on instructions from an assignment provided by Networkapp.
- The assignment provided by Networkapp primarily consists of the processing of personal data and the services of the external party are aimed at this.

If on the basis of the aforementioned standards it is established that there is a processor and the **main purpose** of the assignment is focused on the processing of personal data, then Networkapp, as the controller, draws up a written processor agreement.

Networkapp maintains a central administration of all processor agreements.

[1] The GDPR (Dutch: AVG) uses the Dutch name data protection by design and by standard settings, but since the English-language equivalent is common in daily use, this is also used in this document.

H. Behavioural codes and certification mechanisms

Specific codes of conduct concerning the processing of personal data are not (yet) available. We strive to comply as well as possible with quality frameworks in the field of information security, such as NEN 7510, 7511 and 7512.

RIGHTS OF PERSONS INVOLVED

A. Informing person concerned

People concerned, the employees, customers and users of Networkapp, have the right to know what happens to their personal data and why. They must also be made aware of the risks of data processing, the rules that apply to them, the safeguards and the way in which they can exercise their rights with regard to the processing of personal data.

Networkapp informs the data subjects when the personal data are collected from them, but also when the personal data are collected outside the data subject. The person concerned will be informed about the way in which personal data are processed by means of a privacy statement on the various websites of Networkapp and in the Networkapp.

Networkapp aims to provide all information necessary to ensure proper and transparent processing with regard to the data subject. If Networkapp decides to process personal data already collected for a purpose other than the one for which it was obtained, the data subjects will again be informed about this. Obviously, in such a case, processing personal data for the new purpose must be compatible with the original purpose.

B. Right to inspect

Every person concerned has the right to inquire whether his personal data are being processed. If that proves to be the case, he is entitled to receive information about what and how, as well as a copy of his personal data, at reasonable intervals. Networkapp will not charge any costs for the provision of one written or electronic copy of its personal data. For possible additional copies, Networkapp charges a reasonable fee based on administrative costs.

It is a requirement for Networkapp that the data subject identifies adequately. Moreover, the personal data provided by Networkapp may not infringe the rights and freedoms of third parties.

C. Right to rectification

If processed personal data are incorrect or incomplete, the person concerned has the right to have these corrected or supplemented by Networkapp. This right can be exercised to correct obvious factual errors.

D. Right to removal (‘right to be forgotten)

Networkapp removes, under certain circumstances, at the request of people concerned, their personal data when they exercise the right to do so. The 'right to be forgotten' was especially created to not confront people on the internet with their past forever. Networkapp is obliged to comply with requests for

the right of removal, except when the data are processed on the basis of a legal obligation and to substantiate legal claims.

When Networkapp has shared deleted data with other parties, it will inform them of the removal(s). Except when this proves impossible or in the opinion of Networkapp would require a disproportionate effort by Networkapp.

E. Right to restriction

This offers the person concerned the opportunity to temporarily "stop" the processing of his personal data until a problem or objection has been resolved. If the application to limit the processing by Networkapp is honoured, then Networkapp must determine for itself how the processing of the personal data in question will be temporarily suspended. However, in some cases Networkapp must indicate (make visible) that the processing of personal data is limited.

F. Right to objection

Under certain circumstances, Networkapp must cease processing of personal data if a data subject exercises his right of objection. The person concerned can do this in three situations:

1. Based on personal circumstances if the processing is based on the grounds that:
    a. is necessary for the performance of a task of general interest; or
    b. is necessary for representing legitimate interests of Networkapp.

    If, on reassessment, it appears that the privacy interest of the person concerned is greater than the legitimate interest of Networkapp, then Networkapp will have to discontinue the processing of personal data concerned.

2. When processing personal data with a view to direct marketing.
    In this case, the right to object is absolute and Networkapp is obliged to discontinue the processing of the personal data concerned.

3. When processing personal data for scientific or historical research or for statistical purposes. Networkapp must also comply with this objection, unless the processing is necessary for the performance of a task of general interest.

G. Right to transfer of data ('data portability')

This right is in fact an extension of the right to access and offers the person concerned the opportunity to obtain a copy of the personal data he has provided to Networkapp. Networkapp offers the copy in a structured, current and machine-readable form, with the aim of facilitating a switch to another service provider or provider for the data subject.

The right of transferability **only** applies to *provided* data that are processed *automatically* on the basis of the following principles:

- the unambiguous or express consent of the person concerned;
- the necessity for the execution of the agreement.

The concept of personal data *provided* does not only include data that the data subject himself provided when submitting a report via the web or on paper, but also the data that are observed by the data subject, such as behavioral data registered by *cookies* (https://networkapp.eu/nl/cookie-statement/), such as

interpretations or conclusions drawn by Networkapp on the basis of the data are not covered by the right to transfer.[2]

Networkapp is not obliged to accept the personal data provided by a data subject and provided by another provider.

H. Right not to be subject to automated individual decision-making

Automated individual decision-making takes place when personal data are used to reach a certain decision and there is no question of human intervention (which is noteworthy) so that any outcomes can be corrected.

Examples of this are profiling: the classification of people into categories (profiles) on the basis of their personal data. Based on these profiles, (automated) individual decisions can then be taken.

Individuals have the right not to be subject to a single on automated processing based decision when this:

- has legal effects for them; or
- it otherwise affects them to a considerable extent.

In fact, this is not a right for the person concerned, but a ban for Networkapp. However, there are also forms of automated individual decision-making that have legal consequences for those involved or significantly affect them, but are nonetheless allowed.

CONSERVATION OF COMPLIANCE WITH PRIVACY LAW

The environment in which personal data are processed is permanently subject to change. In this ever-changing world, the processing of personal data remains undiminished. In this respect, it is important that a level of compliance once achieved is at least maintained and that this can also be demonstrated. Networkapp therefore conducts an assessment at least once a year.

[2] This is the opinion of the Article 29 Working Party and not necessarily of the European legislator.