Privacy protocol AEZEL

Date: June 7, 2021, version 1.1.

The General Data Protection Regulation (GDPR) came into effect on 25 May 2018. One and the same privacy legislation will then apply throughout Europe.The GDPR applies to anyone who keeps personal data that is not public. Personal data is all data that can be traced back to a person. Examples of this are name, address, e-mail, telephone number, gender and IBAN.

For AEZEL this is the data of

- volunteers who contribute to AEZEL. This can be through an archive or heritage organization or directly. Personal data is registered for mutual communication and authorization in the automated administration.
- relationship files of persons who have indicated that they wish to be kept actively informed of information about AEZEL, via newsletters
- data from users of the website

In the appendix (following) it is stated which personal data AEZEL registers. It is necessary to consider the purpose for which the data is collected, how it is stored and who has access to it. The aim is to optimally monitor privacy.

In this inventory we have recorded who is responsible for the data, how it is stored, who has access and how it is protected against viruses and hacking.

The personal data will only be used for the purpose for which they are intended. They are never passed on.

The LGGI board will account for the implementation of this Privacy Policy in the annual report.

Assumptions

AEZEL handles personal data in a secure manner and respects the privacy of those involved. AEZEL adheres to the following principles

1. Legality, fairness, transparency
Personal data is processed in accordance with the law and in a proper and careful manner.

2. Basis and purpose limitation
AEZEL ensures that personal data is only collected and processed for specified, explicit and legitimate purposes. Personal data will only be processed on a fair basis.

3. Data Minimization
AEZEL only processes the personal data that are minimally necessary for the predetermined purpose. AEZEL strives for minimal data processing. Where possible, less or no personal data is processed.

4. Retention period
Personal data is not kept longer than necessary. The retention of personal data may be necessary to be able to perform the tasks properly

5. Integrity and Confidentiality
AEZEL handles personal data with care and treats it confidentially. For example, personal data is only processed by persons with a duty of confidentiality and for the purpose for which this data was collected. In addition, AEZEL takes appropriate measures to protect personal data.

6. Security
AEZEL has taken appropriate technical and organizational measures to protect personal data against unlawful processing:

- All persons who can take cognizance of personal data on behalf of AEZEL are bound by the confidentiality thereof;
- AEZEL has a username and password policy on all systems;
- AEZEL makes backups of personal data in order to be able to restore them in the event of physical or technical incidents;

7. Rights
Persons have the right to inspect, rectify or delete the personal data that AEZEL has received from these persons. You can also object to the processing of this personal data (or part of it). AEZEL may ask people to identify themselves before being able to comply with the aforementioned requests. If AEZEL processes personal data on the basis of permission to do so, the person concerned always has the right to withdraw this permission.

8. Complaints
If persons have a complaint about the processing of their personal data, they can contact AEZEL directly. Individuals always have the right to file a complaint with the Dutch Data Protection Authority, the supervisory authority in the field of privacy protection.

9. Data leak procedure
We speak of a data breach if personal data falls into the hands of third parties who should not have access to that data, for example leaked computer files or a lost printed list or USB stick.

A data breach is reported to the chairman of LGGI within 72 hours of discovery, who will record the report

- the nature of the infringement;
- the authorities or person from which more information about the infringement can be obtained;
- the recommended measures to limit the negative consequences of the infringement;
- a description of the observed and suspected consequences of the breach for the processing of personal data;
- the measures that the organization has taken or proposes to take to remedy these consequences
- whether the seriousness of the leak is such that a report must be made to the Personal Data Authority via http://datalek.autoriteitpersoonsgegevens.nl

10. Questions
If you have any questions or comments regarding our privacy policy, please contact the secretary of the LGGI (s