VESA - Privacy Policy

Last update : July 2026

PREAMBLE

Veolia Environnement SA (VESA) attaches particular importance to the protection of personal data, and intends to comply in all respects with applicable regulations.

This Privacy Policy aims to inform any natural person concerned (collaborators or candidates, clients, suppliers or partners and their employees) of the way in which their personal data is processed when VESA collects it, uses, stores, and shares them in the exercise of its activities.

It also aims to inform its employees and subcontractors of the rules and principles to be followed in order to ensure that personal data is processed in accordance with applicable legislation on personal data, in particular the General Data Protection Regulation (No. 2016/679) (hereinafter the "GDPR") and the Data Protection Act No. 78-17 of 6 January 1978. As such, it is likely to evolve according to needs, due to the legal context, in France or within the European Union, as well as recommendations or decisions of the French data protection authority (the CNIL).

This Policy covers all services and content, whether in paper or digital form, provided that VESA acts as the controller of the personal data involved.

This Policy applies only to VESA. It does not apply to data processing operations carried out by third parties as data controllers or other entities within the Veolia group, which are also required to adopt their own personal data protection policy.

1. GOVERNANCE

VESA has set up an organization responsible for compliance with this Policy and the GDPR under the control of the Data Protection Officer (hereinafter "DPO") attached to the Group Compliance and Security Department. This approach is based on internal procedures and ongoing awareness-raising among its employees, ensuring that data protection is taken into account before any new processing of personal data is implemented.

2. FUNDAMENTAL PRINCIPLES

2.1 Lawfulness, fairness and transparency regarding the individuals

Any personal data processing is justified by a legal basis: the pursuit of VESA's legitimate interests, the fulfillment of a legal obligation to which VESA is subject, the consent of the data subject or the conclusion or performance of a contract between VESA and that person. The legal basis applicable to data processing is indicated in the relevant privacy notice.

Personal data is processed within the limits of what will have been described in the privacy notice that

accompanies each processing operation regarding: the identity of the controller, the purposes pursued by the envisaged processing, the methods of its implementation, the recipients with whom the data may be shared, and the retention period of the processed data. If personal data is collected indirectly, the source of the data will be specified.

This clear information allows informed consent when consent is the legal basis for data processing, and helps to exercise one's rights on its personal data. The data subjects thus have a right of access and rectification enabling them to update information that is no longer up to date, as well as a right to portability allowing them to receive their data in a structured format, commonly used (Excel spreadsheet file for example) and readable to forward them to another manager. They may also oppose the processing of their data for reasons related to their own situation, this right being unconditional in terms of commercial prospecting. The right to erasure of data is guaranteed as soon as it is no longer indispensable, while withdrawal of consent for processing that requires it is possible at any time without negative consequences. Finally, the persons concerned can indicate to VESA their guidelines regarding the methods of storage, deletion and communication of their personal data to be taken into account after their death, or submit a complaint to the CNIL if they believe that their rights are not being respected. The precise list of applicable rights for each treatment is indicated in the corresponding privacy notice.

To exercise these rights, each data subject may send an email to the address dpo.vesa@veolia.com. Upon receipt of a request to exercise the right, VESA will respond within one month maximum for simple requests, and three months maximum for complex requests that involve a large amount of data.

All received requests to exercise rights are centralized in a register in order to document the date and type of response.

2.2 Purposes limitation and data minimization

As a data controller within the meaning of the GDPR, VESA bears the responsibility for the data collected:

- directly with the data subject: when this person fills in electronic or paper forms, subscribes to online services, uploads content online, or sends emails, paper letters, etc. to VESA;
- or indirectly to third parties via public or non-public sources: if applicable, VESA will communicate, at the time of the first communication, all information on the processing and the source of the data.

VESA collects personal data in strict compliance with specified and explicit purposes, and will not reuse it in a way that would be incompatible with the initial objectives of its collection. The list of data collected as well as the purposes pursued for each treatment are indicated in the relevant information notice.

All personal data processing implemented by VESA is described by the DPO of VESA in the "Data processing Register" in order to document and ensure that each data processing complies with the rules for data protection.

2.3 Accuracy of the data used

In order to ensure that the personal data processed is accurate, VESA takes the necessary measures to rectify or erase without delay any personal data that proves to be inaccurate.

2.4 Time-limited retention of data

VESA strives to limit the retention of personal data according to the applicable purposes and limitation periods. The personal data is then permanently deleted or anonymized. VESA may retain certain personal data for a legitimate reason, for example if VESA believes that fraud has been committed, or when required to do so by law. The retention periods applicable to data processing are indicated in the relevant privacy notice.

2.5 Protecting the integrity and confidentiality of data

VESA implements security measures proportionate to the risks and sensitivity of the data in order to preserve its availability, confidentiality and integrity. To this end, VESA's IT teams or their subcontractors implement the requirements of VESA's cybersecurity policy, in particular those relating to:

- the identification of cyber risks,
- the implementation of appropriate network protections, via filtering devices,

- maintaining the various infrastructure and application components in safe condition, including applying security updates and upgrading components to avoid using non-maintenance components,
- the hardening of infrastructure components such as servers or workstations,
- regular verification of infrastructure or application vulnerabilities through monitoring and the use of technical or application vulnerability scanners,
- encryption of data at rest when necessary and in transit,
- the use of good security practices during the development of applications, particularly for web-based applications, the use of the OWASP repository,
- the assignment of user rights respecting the rule of least privilege and the right to know,
- access protection by implementing strong authentication mechanisms, using SSO (Single Sign On) based on the digital identity repository of the Veolia group, and regularly reviewing accounts,
- supervision of the security of personal data and applications accessing it, notably via centralization and use of logs,
- the preservation of evidence proving the implementation of the above measures.

In the event of a breach of personal data held by VESA, all employees are required to notify the incident immediately. As soon as aware of the event, VESA has a dedicated team capable of reacting without delay to, on the one hand, and if necessary, inform the CNIL and, if applicable, the persons concerned and, on the other hand, identify failures and implement appropriate safety measures. Regardless of the scale and severity of the incident, personal data breaches are documented in a dedicated log describing the nature of the breach, its likely consequences, as well as the measures taken or envisaged to prevent a recurrence of this incident or to mitigate possible negative consequences.

3. RECIPIENTS AND TRANSFERS

The personal data processed by VESA are intended only for persons, entities or organizations that, through their missions or functions, may legitimately process them within the limits necessary to carry out the tasks entrusted to them. The list of categories of recipients of personal data is specified in the information notice of the relevant data processing.

3.1 Veolia intra group recipients

Personal data may be accessible to **VESA departments** that have an interest in knowing it for the performance of a specific and determined mission. These may include, in particular, the Internal Control and Audit department, the Compliance and Safety department, the Legal department, the DPO, and the people responsible for handling reports of behaviors that violate the group's ethical rules, as well as to any other internal recipients. All such recipients are subject to compliance with this Policy.

Personal data may be shared with other **legal entities within the Veolia group** if it is necessary in order to achieve the purpose of the processing. These transfers are covered by the appropriate legal instruments.

3.2 External recipients

VESA doesn't sell any personal data. Personal data may be accessible to VESA's business partners, service providers, suppliers or subcontractors if it is necessary in order to achieve the purpose of data processing, including cloud storage platforms. For certain data, the recipients may also be professional bodies, professional mediators, guarantee funds or even the relevant ministries, authorized public bodies, and courts. In the event of a change in control of VESA or the transfer of all or part of its assets, VESA will be authorized to transfer personal data to the new controller.

Regarding those recipients external to the group, VESA contractually requires that they act in accordance with applicable laws and regulations and within the agreed contractual limits. Before the signing of a contract involving the sharing of personal data, preliminary checks are carried out to ensure that the subcontractor required to process personal data in the name and on behalf of VESA is able to protect it. VESA's contracts with its subcontractors provide for the establishment of measures to ensure a level of protection of personal data equivalent to this Policy and compatible with the requirements of the GDPR, notably by physical measures, rigorous and adapted technical, organizational and procedural measures to ensure the availability, confidentiality and integrity of personal data. The contracts also ensure that the subcontractor, supplier, service provider or other third party will not reuse the data for a purpose different from that for which VESA had

entrusted them.

3.3 International data transfers

Some of the aforementioned recipients may be located outside the European Union or the European Economic Area (EEA). In this case, data transfers outside the EEA are governed by the appropriate legal instrument for the recipient country: either the country ensures an adequate level of protection under the GDPR and benefits from an adequacy decision from the European Commission, either VESA signs with the provider located in a non-adequate country standard contractual clauses (CCT) from the European Commission.

CONTACT

Any questions regarding this Policy may be addressed to the DPO by email at dpo.vesa@veolia.com.