

Veolia Environnement SA

Personal Data Privacy Policy

November 2019

1. PREAMBULE

Veolia Environnement SA (VESA) undertakes strong commitments to the protection of personal data placed at the heart of its concerns.

This Personal data privacy policy is intended to inform physical persons (employees, candidates, clients, providers or partners and their employees) on the measures implemented by VESA when collecting personal data in the course of its activities.

This Policy may evolve from time to time, either due to the legal context in France and in the European Union or to recommendations or decisions made by the CNIL (French supervisory authority for the protection of personal data).

This Policy concerns only Veolia Environnement SA; the other entities of the Veolia Group are required to adopt their own personal data privacy policy.

2. PERSONAL DATA COLLECTED, PURPOSES OF THE PROCESSING AND THE DPO

VESA has set up an organization responsible for the correct application and the compliance with this policy, under the supervision of the Group Chief Compliance Officer (“Group CCO”).

Furthermore, VESA takes actions to raise the awareness of its employees to the necessity of protecting personal data so any collection or processing shall not operate unless relevant for the intended purposes and unless such purposes are defined to guarantee they are lawful, specified, explicit and legitimate.

Any processing implemented by VESA that may contain personal data are the subject of a full descriptive form, entered in the “Record of processing” held by VESA’s Data Protection Officer (DPO).

VESA’S DPO thus ensures that the collection of personal data and their processing complies with:

- regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) and
- law n° 78-17 of 6 January 1978 on the protection of personal data (French Data Protection Act).

VESA has placed its DPO under the Group CCO’s authority in a view to guarantee their independence and to put the protection of personal data at the center of the company’s organizational structure.

3. GOLDEN RULES

VESA relies on 6 golden rules so that any person collecting or processing personal data on its account:

- abides by the GDPR and ensures that personal data are collected, used and shared while respecting the rights of the concerned persons and the concept of “*privacy by design*”;
- is transparent and clear with the concerned persons about the purposes of the processing, about the purpose and means of its implementation and about the persons with whom their data will be shared; seeks the natural’s persons consent every time it is possible and proceeds without their consent only where GDPR or the law allows it or where their prior consultation is impossible or may present a specific risk;
- seeks advice in case they have any doubt on how to process any personal data, confronts opinions with other practitioners, gets a legal advice or an advice from the competent supervisory authority if need be and documents their decision;
- bases the decision to collect, use or share personal data on the physical person’s interest in order to process only necessary, relevant, adequate, proportionate, accurate, timely and secure data for a period of time in conformance with the purposes of the processing;
- ensures that any information shared is strictly necessary to reach the purposes of the processing and to allow providers to render the services expected;
- makes sure that the security measures are proportionate to the risks involved and taken to preserve the availability, the confidentiality and the integrity of the processing.

4. CONCERNED PHYSICAL PERSON’S INFORMATION

In accordance with GDPR, VESA is committed to informing the concerned physical persons of the rights they are guaranteed by informing them about:

- the identity of the data controller;
- the purpose of the processing;
- where relevant, whether answers are obligatory or optional and what the potential consequences of their failure to answer are;
- the recipients of the data;
- their right to access, to rectification or to erasure on the data that concern them, the right to object to the processing for legitimate reasons, or to object to the processing of their data for marketing activities as well as the right to provide general or specific instructions for the processing of the data that concern them after their death;
- the period of time for which the data are stored.

5. GROUP PROCESSING

VESA informs all concerned physical persons that the personal data entered into an automated processing are listed in a Register and may be accessed by VESA’s internal audit, by the compliance department or the DPO, by the auditors, by people in charge of instructing alerts on behaviours that may violate the Group’s ethic rules

and by its counsels or a competent authority and, in some cases, by the stakeholders involved in a merger or acquisition.

6. RECIPIENTS

VESA may share some of the personal data collected with Group employees or with service providers and suppliers, strictly within the necessary limits required for the fulfilment of their tasks.

VESA ensures that they comply with the laws and regulations applicable for the protection of personal data and that they pay a special attention to their confidentiality.

7. STORAGE

Personal data collected by VESA or on its behalf are stored by VESA or its service providers particularly on cloud storage services.

For reasons, mostly technical or linked to VESA'S international dimension, some data may be stored or accessed outside the European Union or the European Economic Area (EEA) territories. If so, VESA ensures that effective measures, compatible with the GDPR's requirements, are taken to offer an adequate level of protection for personal data in particular strict and appropriate physical, technical, organizational and procedural measures to ensure the availability, the security and the integrity of the personal data modulated depending on their nature or sensitivity.

VESA seeks to limit the storage duration of personal data to the period of time necessary to complete the operations for which they have been collected and processed as permitted by the applicable regulation. Personal data are then irreversibly destroyed or anonymized.

8. SECURITY AND ALERTS

VESA has adopted measures to ensure the security of the personal data collected in a manner that is appropriate to their sensitivity and to the attached risks. Thus, the IT teams and their providers or their subcontractors implement the requirements set out in Veolia's Cybersecurity policy in particular those relating to:

- the identification of cyber risks,
- the implementation of adapted network protections through filter devices,
- the maintenance in security conditions of the various infrastructure components, in particular, application of the softwares updates and upgrading of the components to avoid their use for other purposes than maintenance,
- the enhancement of the infrastructure components such as servers or workstation,
- regular checks of the infrastructure or applications vulnerabilities by monitoring and using a scanner of technical or applicative vulnerabilities,
- the encryption of the data at rest when necessary and of data in transit,
- the use of security good practices when developing new applications, in particular web applications, use of OWASP guidelines,
- the allocation of users rights complying with the "lesser duty" rule and the right to be informed,
- an access protection by implementing strengthened identification mechanisms and by a regular review of the accounts,

VESA Personal Data Privacy Policy

November 2019

- the security supervision of the personal data and application through the centralization and use of logs,
- the preservation of factors proving the implementation of the above measures.

When a breach affects personal held by Veolia, Veolia will act promptly after it has knowledge of such breach in order to inform the CNIL where appropriate and, if need be, to identify the flaws and implement adapted security measures.

9. PHYSICAL PERSONS' RIGHTS

In accordance with the personal data protection act of 6th January 1978, as modified, physical persons whose data are collected have, within the limits of the law, a right to access, to rectify, if applicable to portability and to erasure of the personal data that concern them and a right to limitation.

They also have a right to give the data controller instructions concerning the fate of their personal data after their death.

Each physical person concerned by a processing may exercise their rights by writing to the person in charge at VESA of that specific processing whose identity was indicated at the moment the collection occurred then by sending an email to VESA'S DPO using the following address: dpo.vesa@veolia.com. If they believe the response is not satisfying, the concerned persons may refer to the CNIL.

10. CONTACT

For any further information relating to this policy, please send a mail or email to VESA's DPO (dpo.vesa@veolia.com) or contact the Group Chief Compliance Officer.

In general terms, any concerned person always has the possibility to contact the French supervisory authority (<https://www.cnil.fr> or to the following address: 3, Place de Fontenoy, 75007 Paris - France).