Group Guidelines for the Adoption of a Personal Data Privacy Policy

November 2019

Veolia strongly believes that the respect of the privacy and the protection of personal data are a cause of great concern and a mean to create trust. In that perspective, Veolia has decided to adopt those guidelines that will have to be implemented in all the Group's entities in order to set some common rules for the protection of personal data.

Entities that do not meet the material or geographical criterias for the application of GDPR must apply the Group Minimal Standards as stated in "GDPR for Group entities located outside the EU" ("Non GDPR entities") attached to these Guidelines.

1. Scope

Each of the Group entities must establish a Personal Data Privacy Policy.

Veolia Environnement SA's Personal Data Privacy Policy constitutes a common standard for all Group entities; this standard must be used by all entities as soon as they receive notification of VE SA's Policy, with the exception of the entities having to adopt a modified version, subject that such modifications:

- are made mandatory due to:
  - local laws, in particular employment or personal data protection laws,
  - binding decision from the local supervisory authority in charge of ensuring the protection of personal data contained in files or processing, whether the processing is private or public,
  - specific features of the entity's activities,
- shall be validated, prior to their adoption, by the group CCO or the person(s) the CCO may have designated to this effect.

2. "Golden rules"

Each entity must incorporate at least the six following Golden Rules in their Personal Data Privacy Policy so any person collecting or processing personal data on their account:

- abides by the GDPR and ensures that personal data are collected, used and shared while fully 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 proposed processing, about the purpose and means of its implementation and about the persons with whom their data will be shared; seeks the physical 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 expected services ;

- 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.

3. Data Protection Officer (DPO)

Each Veolia Zone must appoint a Zone Personal Data Correspondent (Zone PDC), including in countries where Veolia operates even if not in the scope of GDPR: the Zone DPC will be the Group's contact for the whole Zone on all issues related to personal data and monitors the zone compliance with these Guidelines.

In France, a DPO is appointed for each Business Unit (BU).

The Zone PDC or the BU DPOs have the possibility to appoint one or several local DPOs (or correspondents) where the organization of their Zone or BU or the local legislation may require so; they may also appoint one or several "Data Protection Managers" (DPM) to assist them in their duties and functions.

The Zone DPC will act as DPO for the zone entities or as local DPM in case they fail to proceed with required appointments.

Each Zone PDC acts independently and reports directly to the Local Chief Compliance Officer (Local CCO) or to the highest level of the zone's hierarchy if a Local CCO is not appointed.

4. Customers' Personal Data

Should an entity's business bring the need to collect physical persons personal data, as direct customers or as beneficiaries of a public service, this entity's Personal Data Policy will set the special measures put in place for their benefit.

5. Security

The entity shall adopt the measures to ensure the processed personal data security is adapted to their sensitivity and to the risks attached to the processing, including with its subcontractors.

In this regard, the entities will need to comply with the Group Security Department's policy "PO-TSE 11 *Veolia GDPR Security policy* " -as it may be amended from time to time- forming an appendix with the Data Privacy Policy.

Addendum to the Group Guidelines for the Adoption of a Personal Data Privacy Policy
- Applicable to Non GDPR Group Entities -

Each Non GDPR Group Entity must establish a policy for the protection of personal data, taking account of the "Golden Rules" and to the extent possible based on the common standards applicable to GDPR Group entities included in VE SA's Data Privacy Policy. In particular, Non GDPR Group Entities must, subject to more restrictive local laws and regulations (**see attached summary in table below**):

- implement a Record of processing relating to :
    - i) their employees (wages and salaries, career management, health protection, provision of professional equipments and tools),
    - ii) the contractual relation with their clients (services and goods provided, billing information),
    - iii) the contractual relation with their providers (management of contracts, billing information),

- in the Record of processing, identify the list of categories of data collected and their recipients; restrain from sharing personal data where not made mandatory by law or to reach the purposes of the processing; to the extent possible, adapt their contracts to secure shared data,

- limit the data collected to what is strictly necessary to complete the purpose of the processing and erase all irrelevant data; restrain from retaining data for an unlimited duration; abstain from processing sensitive data when not compulsory,

- inform data subjects that the collection of their data will be limited to what is strictly limited to reach the purpose of the processing and that security measures have been adopted in compliance with the Group Security Department standards. Such information can be provided on the internet website or in any manner the Group Non GDPR Entity deems appropriate and compliant with local laws,

- to the extent possible, make the information available that a person has been appointed that any concerned person may contact for questions relating to the processing.

	Group GDPR Entity	**Group non GDPR Entity**
Appoint a DPO	X	*optional* *(at a min a DPC or a DPM)*
Implement a data privacy policy compliant with VESA's	X	
Implement a data privacy policy		X
Implement a record of processing	X	X
Implement a DPIA tool	X	
Monitor a DPIA when sensitive data are collected	X	
In the Record of processing: ● be transparent on the purposes	*detail all purposes*	*main purpose*
● minimize personal data collected	X	X
● list personal data collected	*all*	*categories*
● define an adequate retention period	*strictly limited duration*	*reasonable duration*
● identify the recipients	*all (direct & indirect)*	*main*
● describe data flows	X	
● document data transfers between entities in the EU/outside the EU	*always*	*when a risk is identified*
Where applicable, seek consent of concerned physical person before collecting their data	*each time* *(except cases set out in art. 6.1 GDPR)*	*if feasible or appropriate*
Inform concerned physical person of the processing implementation	X	X
Inform concerned physical person of their rights	*provide all information on their right (access, erasure, portability…)*	
Adopt security measures to protect personal data	*provide proof as set out in art. 32 GDPR & comply with Group security policies*	*Implement Group security policies*
Amend contracts	*insert provisions and appendixes required under GDPR in all contracts (ongoing or new)*	*in all new contracts, insert provisions to ensure the protection of personal data and prevent inappropriate use*