1. Introduction

All Veolia UK & Ireland business entities (herein referred to as 'Veolia' or 'the Company') are obliged to comply with laws and regulations to protect personal data relating to their customers, suppliers, employees and other parties. This policy sets out procedures to ensure compliance in the way Veolia obtains, processes, secures and discloses this personal data across all operations and systems. These procedures include managing actual or suspected disclosure of personal data to unauthorised third parties and responding to Subject Access Requests (SARs) from individual data subjects.

Data protection is a fundamental right of every individual, or data subject. All data subjects are entitled to expect that any personal data relating to them is protected by anyone who holds it. This policy sets out Veolia's commitment to protect personal data.

2. Scope

This policy applies to all personal data in Veolia's possession, including data relating to customers, suppliers, past and present employees, members of the public and other parties.

Data can be defined as information in a form that can be processed. It may be held in manual or electronic records. Personal data is data relating to a living individual who is identified or identifiable from the data either by itself or together with other information.

3. References

3.1 Veolia UK & Ireland Acceptable Use Policy - Details a set of rules to be followed by end users accessing Company computing resources. The policy also provides further data protection guidance for end users.

3.2 Veolia UK & Ireland Data Retention Protocol - Details the framework and recommended data retention periods for personal data and other documentation.

3.3 Veolia UK & Ireland Video Surveillance (CCTV) Policy and associated procedures - Governs how Veolia uses CCTV in a legal and responsible way.

3.4 Veolia Group Cyber/Information Security Policies, including;

- Group IS Security Policy
- Group GDPR Security Policy

3.5 Veolia Group Legal Key 19 - Details Veolia Group's high level data classification, protection and retention strategy.

3.6 Compliance Library - Collection of documents relating to Veolia UKI's compliance with data protection and information security requirements.

4. Definitions

None.

5. Policy

5.1 Policy Statement

Veolia collects and processes personal data relating to customers (including domestic water and energy customers), suppliers, contractors, municipal contract residents, employees (both past and present) and in some cases members of the general public. Personal data can include (this list is non-exhaustive):

Name	Next of kin
Occupation	Employee ID
Address	Gender
Banking information	Telephone number
Date of birth National insurance number	IP address
	Images [inc. CCTV]

Veolia has legal and ethical responsibilities to safeguard the personal data of data subjects in its possession. Veolia is bound by the requirements of the General Data Protection Regulation (GDPR) (2016) and other relevant laws and regulations, some of which are detailed in the References section of this policy. Veolia UK remains bound by the 'UK GDPR', even after leaving the European Union.

In particular, Veolia is committed to complying with the principles of data protection as set out below. Personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Failure to comply with this policy will lead to non-compliance with Veolia's legal and regulatory obligations, potentially exposing individuals to prosecution and the Company to the following risks:

- Imposition of significant fines (up to 4% of Veolia's global turnover) by the UK Information Commissioner's Office (ICO), the Irish Data Protection Commissioner (DPC) or other relevant supervisory authority
- Civil claims by data subjects
- Additional costs associated with management of personal data breaches; and
- Reputational damage to the Company and the Veolia Group

As part of our ongoing commitment to ensuring compliance, Veolia has produced a detailed Information Security

and Data Protection Roles and Responsibilities Document, available here.

The main roles and responsibilities within Veolia, in relation to data protection are as follows;

Executive Vice President (UK & Ireland) - responsible for ensuring that the policy is fully implemented by Veolia in all its operations.

Data Protection Officer / Team - responsible for policy content and communication to all Company operations and policy updates as required. Responsible for monitoring and advising on compliance with data protection legislation.

Personal Data Users - responsible for ensuring that personal data processing activities are reported to the Data Protection Team, so they can be included within our Records of Processing Activities, and that any new purposes for which personal data is processed, or new classes of data subject or parties to whom disclosure will be made, are notified to the Data Protection Team for inclusion in an updated register entry.

Veolia IS&T Product Owners - responsible for ensuring that information systems used to process personal data maintain appropriate technical and organisational measures proportionate to the types of personal data under processing.

Employees - responsible for ensuring that they understand the implications of this policy for their roles, and comply with the policy.

5.2 Training and Audit

Veolia provides appropriate annual training for all employees who have access to its records and systems and, in particular, personal data. This ensures that all employees are aware of the legal and ethical requirements and their responsibility to comply with them.

Ad-hoc, and more specific training may be conducted by the Data Protection Team. This training can be designed and delivered by the Data Protection Team upon request from a Veolia function.

The Data Protection Team conducts periodic audits of Veolia functions and operations, to monitor and ensure compliance with data protection legislation and best practice. Veolia functions and operations may also choose to conduct internal audits of their own departments. For advice on how to conduct these audits, the Data Protection Team may be consulted via UKI.GDPR@veolia.com.

5.3 Privacy Notices and Lawful Bases

All data subjects must be provided with a Privacy Notice before their personal data is collected or processed. A Company-wide Employee Privacy Notice is provided to all staff. If you require a privacy notice for purposes of collecting personal data from customers, suppliers, members of the public or any other party, please seek guidance from the Veolia Data Protection Team at UKI.GDPR@veolia.com.

When processing personal data, we must identify a 'Lawful Basis'. These bases are laid out in the GDPR / UK GDPR and are as follows;

- We have the consent of the data subject (see section 5.4 of this Policy)
- We are required to process the data for the performance of a contract with the data subject (or it is required to enter into a contract with them)
- We are legally obliged to process the personal data
- It is in the data subjects' vital interest to process the data

- It is necessary for the performance of a public task to process the data
- It is within our legitimate interests as a business to process this data (provided that those interests are not overridden by the interests of the data subject).

Veolia's Data Protection Team records the lawful basis for every processing activity within our Records of Processing Activities. For more information / guidance on which lawful basis is applicable, contact UKI.GDPR@veolia.com.

5.4 Data Subject Consent

Where Veolia seeks to gain a data subject's consent to process their personal data, certain criteria must be met:

- Consent must be knowingly and freely given. It must also be clear and specific to the intended purpose.
- Consent cannot be the 'default option' e.g. a pre-ticked box, or a "tick to opt-out" option.
- There must be a clear and simple way for the data subject to withdraw consent, and they must be informed of this prior to giving their consent.
- Data subjects should be able to refuse or withdraw consent without detriment.
- Consent should be recorded, including what processing the data subject consented to.
- Consent should be regularly reviewed to check that the relationship, processing or purposes have not changed.

5.5 Special Category (i.e. Sensitive) Data

Where Veolia processes special categories of personal data, we require a lawful basis (Section 5.3 of this Policy) **and a further condition of processing**. Veolia may rely on the explicit consent of the data subject, but may rely on other legal bases such as; employment law/occupational health, vital interests or the establishment / exercise / defence of legal claims.

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Sex life or sexual orientation
- Gender other than that assigned at birth (this isn't explicit in legislation, however has been confirmed by Supervisory Authorities).

Criminal offence data may only be processed in an official capacity, or with specific legal authorisation.

5.6 Data Subject Rights

Data subjects have a number of rights in relation to their personal data, including to:

- be informed about use of their personal data
- access their personal data
- correct their personal data
- erase their personal data
- restrict data processing

- object to data processing
- not be subject to automated decision making
- be notified of a data security breach

There are limits and exemptions to all of these rights, therefore any request from an individual to exercise any of these rights should be completed via OneTrust and assessed by Veolia's Data Protection Team.

5.7 Data Protection Impact Assessments and Data Protection by Design and by Default

All projects, systems, processes or procedures which involve personal data processing shall be reviewed to determine whether a data protection impact assessment (DPIA) is required. A DPIA is required in situations where the personal data processing activity may present a risk to the data subjects, for instance where the processing involves information such as medical details.

Veolia aims to implement appropriate technical and organisational measures which demonstrate that data protection is integrated into personal data processing activities. Every new project, system, process or procedure that will involve personal data processing should ensure that the principles of data protection by design and by default are incorporated.

For guidance on the principles of data protection by design/default, and when/how to conduct a DPIA please contact the Data Protection Team at UKI.GDPR@veolia.com. A *"Do I need to do a DPIA?*" form can be completed directly via the OneTrust Self Service Portal.

5.8 Marketing and the PECR

Where Veolia uses direct email marketing targeted towards individuals (rather than businesses/organisations), the Privacy and Electronic Communications Regulations (PECR) applies. Direct email marketing to individuals should only ever be conducted where Veolia has received clear and unambiguous consent from the data subject, or through a 'soft opt-in' which occurs when the data subject is an existing customer who bought (or negotiated to buy) a similar product or service from Veolia in the past. Where consent is sought, it must comply with the "Data Subject Consent" section (5.4) of this Policy.

Every communication which can be considered as marketing, should give the data subject a simple way to opt-out of further marketing communications. If the data subject uses that opt-out, they must never receive email marketing from that source, unless they later indicate otherwise.

5.9 Transfer of data outside the EEA

Veolia may transfer UK personal data outside of the UK (some transfers may be to the EEA, some may not). Where this is the case, Veolia will ensure that adequate safeguards are in place. Veolia will also have suitable transfer mechanisms with Veolia entities within the EEA, including Veolia Ireland Entities and Veolia Group (based in Paris).

Veolia may occasionally transfer EEA personal data outside of the European Economic Area (EEA) for legitimate reasons. Veolia will put adequate safeguards in place to ensure that the recipient of the data complies with applicable data protection requirements.

5.10 Data Processors

Veolia may use third parties to process personal data on its behalf for legitimate business reasons. In this event, Veolia will ensure that appropriate contracts are put in place which commit the third party to process the personal data in accordance with Veolia's instructions and in accordance with legal and regulatory requirements.

Veolia may disclose personal data to professional advisors, credit reference agencies and other parties for

legitimate business reasons, under conditions of strict confidentiality.

5.11 Breaches, Non-Compliance and Escalation

All Veolia employees are responsible for identifying matters of non-compliance or potential non-compliance with this policy, including personal data breaches. Any such matter must be reported immediately via the OneTrust Self Service Portal using the "Breach Report" form. You should preserve all evidence while the matter is being investigated.

A personal data breach occurs when there is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data." This includes breaches that are the result of both accidental and deliberate actions.

If you believe that you have discovered something that poses a risk to;

- The confidentiality, integrity or availability of information (including personal data) that Veolia holds,
- Veolia's compliance with our legal or regulatory obligations (e.g. GDPR)

You can report this via the OneTrust Self Service Portal "Report a Risk" form.

The Veolia Data Protection Team will review any reported matters of non-compliance, potential non-compliance or breaches and if confirmed, will prepare an action plan with the relevant business function to remedy the matter within an appropriate time frame. Please do not attempt to deal with a non-compliance or breach without the assistance of the Data Protection Team.

Anyone who wishes to anonymously report either a personal data breach or a security/compliance risk to the Data Protection Team should refer to the Veolia UK & Ireland Whistleblowing Policy (available on the VMS).

5.12 Data Security

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information to which they have access is not disclosed either orally or in writing (accidentally or otherwise) to any unauthorised third party

Physical security is as important as cybersecurity. Where personal data is held in physical (e.g. paper) form, the owner of the processing activity that uses that data must ensure that the data is adequately protected from accidental or unlawful loss, destruction, damage or unauthorised access/disclosure. Security of sites processing (including storing) hard-copy data must be in accordance with the Veolia Physical Security Standard (available on the VMS), and should take into account the volume/sensitivity of the personal data held on site.

Staff should note that unauthorised processing of personal data and/or failure to adhere to the requirements set out below will usually be a disciplinary matter, and may be considered gross misconduct in certain cases.

Personal data should be:

- Kept in a locked filing cabinet or in a locked drawer if it is in hard copy
- If it is computerised, be password protected where necessary
- If held in Google Drive, have appropriate 'share settings' that do not allow for general access
- When kept on portable media (such as USB devices or CDs), all personal data must be encrypted.

Unless absolutely unavoidable, personal data should never be stored at staff members' homes, whether in hard

copy or electronic form, on laptop computer hard drives or other personal portable devices, or at other non-Veolia sites. In cases where such off-site processing is felt to be absolutely necessary, all security guidelines must still be followed.

Personal data stored on electronic devices or removable media is the responsibility of the individual member of staff who operates the equipment. It is the responsibility of this individual to ensure that:

- Suitable backups of the data exist
- Data is appropriately encrypted
- Special Category (Sensitive) data is not copied onto portable storage devices without regard to appropriate encryption and protection measures
- Electronic devices such as laptops, mobile devices and computer media (USB devices, CD's etc) that contain sensitive data are not left unattended at any time.

It is the responsibility of any employee who discovers an area/situation that violates this section of the Policy to report this via the OneTrust Self Service Portal "Report a Risk" form.

5.13 Personal Data Retention and Classification

Data retention rules shall apply to all personal data processed by the Veolia. Personal data can be held in many forms, including:

- Emails
- Paper copies
- Electronic copies
- Images, video and audio

Personal data should only be retained for as long as necessary. The retention periods can differ based on the type of personal data processed, the purpose of processing or other factors. Issues to consider include:

- Whether any legal requirements apply for the retention of any particular personal data?
- In the absence of any legal requirements, personal data may only be retained as long as necessary for the purpose of processing. This means personal data is to be deleted e.g. when:
  - the data subject has withdrawn consent to processing
  - a contract has been performed or cannot be performed any more or
  - the personal data is no longer up to date
- Has the data subject requested the erasure of data or the restriction of processing? ○ Is the retention still necessary for the original purpose of processing?
- Is the data still necessary for the original purpose that it was collected?

For any category of personal data not specifically defined in the Data Retention Protocol, the owner of the process must define a suitable retention period that ensures the personal data is only held for as long as is required to achieve the purpose. This retention period should be documented and justifiable if requested.Once personal data is due for disposal it should be deleted, shredded or otherwise destroyed. The method of disposal will depend upon the nature of the document. For example, any documents that contain particularly sensitive personal data must be disposed of as confidential waste or be subject to secure electronic deletion; whereas low risk personal data may only warrant in-house shredding.

Where necessary, documentation should be classified and labelled in line with Veolia Group's Legal Key 19 under one of the following headlines;

- **Open Data**
  - Freely and publicly available
- **Non-Confidential Data**
  - Data created by Veolia (or an external party) for an internal or external use. Should not be shared externally, unless otherwise authorised.
- **Confidential Data**
  - Data created by Veolia (or an external party). Sensitive data that should not be shared internally or externally.

Where there are specific instructions or restrictions on how a documentation should/can be shared, these should be detailed within the document.

5.14 Review

This policy will be reviewed at least every two years or as required by business requirements, legal or regulatory changes.

5.15 Violations of this Policy

Incidents, actions and behaviours which are determined to be in violation of this policy will be assessed for their severity. Investigating such violations may require the collection and evaluation of user related activity and evidence. Employees must be aware that violations of this policy may lead to disciplinary action, regardless of whether or not the violation is committed during working hours and regardless of whether Veolia equipment/resources or those belonging to the employee are used to commit the violation. Serious violations are likely to also constitute illegal acts/behaviour, as such they may be treated as Gross Misconduct within the disciplinary procedures (of the relevant business unit) and therefore may result in dismissal.

5.16 Further Information

If you have questions or comments relating to any aspect of this policy, please contact your line manager in the first instance. You may also contact the Data Protection Team at UKI.GDPR@veolia.com for further explanation and/or policy guidance.

6. Variation

There are no exclusions or special situations where this Policy does not apply.

7. Documentation

None.