VEON Group Privacy Policy

Policy Owner: VEON Group co-CEOs

Effective Date: 1 January 2021

I. Delegation and GRC Framework/Policies

This Group Privacy Policy ("**Policy**") is part of the GRC Framework established in accordance with Section 3 of the VEON Group Authority Matrix / Delegation (the "**Delegation**"). The Delegation establishes the governance structure of the VEON Group and decision-making authority levels; the GRC Framework and associated Policies supplement the Delegation, establishing processes and other requirements on specific topics. Any questions of interpretation or conflict should be referred, in the first instance, to your supervisor, relevant department head or the relevant OpCo Policy owner and, in the second instance, to the Group Policy owner and legal team.

II. Summary and Purpose

Privacy is the protection of information relating to individuals. The VEON Group is committed to protecting privacy in compliance with applicable data protection laws. This Policy sets out the approach, basic principles, controls and governance regarding the handling, processing and use of Personal Data[1] for the VEON Group. It is the responsibility of each VEON entity to cover this approach and these requirements locally to ensure that all handling, processing and use of Personal Data is carried out in accordance with this Policy and applicable data protection laws. Each OpCo shall at minimum apply the privacy principles for the processing of Personal data as set out in Annex I.

Privacy is a human right and increasingly important in a modern, digital world, especially for a business such as ours. VEON Group's commitment to privacy is therefore relevant to its stakeholders, including its customers, employees, business partners and investors. Accordingly, privacy compliance is and must be an integral part of our business activities.

III. Controls in Place

In order to promote adherence to this Policy and to provide assurance regarding compliance with this Policy and applicable data protection laws, each VEON entity shall maintain and have implemented a Privacy Control Framework. The Privacy Control Framework shall clarify OpCo's standard privacy compliance processes and controls. These controls shall be aligned with this Policy, international standards and best practices for privacy compliance management, and shall at minimum include the baseline privacy compliance processes and controls listed in the example

[1] For VEON EU entities: **Personal Data** shall include any information relating to an identified or identifiable natural person. For each VEON entity outside the EU, **Personal Data** shall have the meaning as specified under local and applicable international data protection laws.

Privacy Control Framework outlined in Annex II. These controls will be reviewed regularly and may be modified to ensure effectiveness as the Policy Owner directs.

IV. Roles & Responsibilities

The Group Policy Owner, OpCo CEO and OpCo CIO/CTO must ensure that an appropriate framework exists at the appropriate level of the organization to protect Personal Data in compliance with this Policy and data protection laws.

The Owner of the VEON Group Privacy Policy is responsible for defining this Policy. OpCo CEOs are responsible for defining and implementing their local Privacy Policy, which references this Policy, international standards and best practices ensuring compliance with applicable data protection laws and fulfilling the responsibilities as set out in Annex III:

V. Confirming Compliance with this Policy

Group Ethics & Compliance, and Group Legal retain the right to review compliance with this Policy. In respect of VEON EU Entities, or those processing Personal Data of individuals in the European Union, the EU Data Protection Officer has the right to conduct reviews or assessments in order to oversee compliance with data protection laws and this Policy.

OpCo management will be required to periodically certify compliance with this Policy, and local and regional management of VEON Group entities may be required to provide assurance on compliance with this Policy. Internal Audit may provide independent assurance to the Chief Executive Officer, Group Chief Compliance Officer and Group General Counsel on effectiveness of and compliance with this Policy.

VI. Applicability and Scope

This Policy applies to the VEON Group, including any director, officer, employee, contractor / consultant, temporary employee or secondee of any VEON entity (collectively, "**VEON Group Personnel**") as well as any agent who is not an employee of VEON or VEON Group, or any other third party properly authorized, instructed or contracted to act for or on behalf of VEON or the VEON Group, whether for the VEON Group as a whole or for one or more businesses in the VEON Group (collectively, "**Authorized Representatives**"). In accordance with the VEON Joint Venture Governance Policy, controlled entities and joint ventures must adopt this Policy as their own or establish a local Policy in line with this Policy to establish the rules/principles set out in this Policy. Additionally, and the VEON Group will use best efforts to ensure compliance with this Policy in non-controlled joint ventures (i.e., entities in which VEON or a member of the VEON Group owns a 50% stake or less).

This Policy and other relevant policies and procedures set minimum privacy compliance standards (based on data protection laws and international best practice for privacy compliance management) that must be followed. Where local laws, regulations, or rules impose a higher standard, that higher standard must be followed. A VEON entity may adopt stricter standards than those set forth in this Policy. All deviations from this Policy must be notified to the Policy Owner, and any deviations that lower standards in this Policy or that otherwise conflict with this Policy must be approved by the local OpCo Board and recorded centrally. OpCo Board approval of this type of deviation is only required if recommended by the OpCo Business Risk Committee.

VII. Where to Go for Help

If you have questions about this Policy, please contact the Policy Owner. If you believe that someone may have violated this Policy, please contact your Local Compliance Officer or Group Compliance at compliance@veon.com. You also may submit a question or concern at www.veon.com/speakup. VEON does not tolerate any form of retaliation, harassment, or intimidation of any person who has reported a concern in good faith.

VEON will investigate alleged misconduct in relation to this Policy under the VEON procedures on investigations. Any VEON Group employee who violates this Policy may be subject to disciplinary measures, up to and including termination of employment.

VIII. Document History

Implementation Date	Revision	Reason/Description
May 2018 for VEON EU Entities November 2018 for OpCos other than VEON EU Entities	1.0	Initial Release
15 August 2018	1.1	Deleted "Question or" (submit a ~~question or~~ concern") from the penultimate sentence of Where to Go for Help section
1 January 2021	2.0	Substantial redraft to reflect changes following from VEON's new operating model

Annex I

Privacy Principles

- **Legal ground**: ensure there is a lawful base (e.g. consent, contract or legitimate interest) for the handling, processing and use of Personal Data;
- **Transparency**: provide appropriate notice to individuals whose Personal Dta is being processed, handled or used;
- **Purpose limitation:** have specific and limited purposes for the processing of Personal Data. Any additional purpose shall be both lawful and compatible with the original purposes for which the Personal Data was collected;
- **Data minimization:** ensure that not more Personal Data is processed than necessary for the relevant purpose;
- **Accuracy:** where relevant, keep Personal Data accurate and up to date;
- **Retention:** keep Personal Data for no longer than is necessary, either by law or for legally justifiable business reasons;
- **Individual Rights**: individuals should be provided with information about, and an easy means to exercise, their rights over the use of their Personal Data;
- **International Transfers**: ensure that there is no transfer or dissemination of Personal Data outside the jurisdiction where it is collected, if not all steps are taken to meet compliance with (local) data protection laws;
- **Third Party Management**: ensure that all third parties and vendors who are handing, processing or using Personal Data on behalf of the VEON Group are properly assessed, comply with our privacy policy, and have signed a contract ensuring adequate safeguards for Personal Data;
- **Security:** keep all Personal Data secure and protect it through adequate technical and organizational measures from unauthorized access, use, alteration, loss, disclosure or transfer, as further defined in the VEON Group Cyber Security Policy;
- **Training & Awareness**: all relevant VEON Group Personnel shall be informed and trained in respect of their obligations to ensure they follow this Policy and OpCo privacy policies when handling, processing and using Personal Data.

ANNEX II

Privacy Control Framework Template

Privacy Control Framework.xlsx

Summarized overview privacy processes and controls

Control Name	**Control Description***
Cross border transfers	Prior to a cross border transfer activity with Personal Data, it is validated if all legal requirements for the transfer are met
Data Inventory	If required by local law: maintain a register/inventory with all processing activities with Personal Data/filing of an OpCo's processing activities at the local DPA
Data subject rights	if local privacy laws include individual privacy/data subject rights (such as right of access, rectification deletion, etc.): maintain a documented process that ensures that individual rights requests are handled timely and compliantly
Governance	Assigned responsibility for privacy compliance. Appointment of accountable privacy control owners as set out in the VEON Privacy Control Framework and the VEON Privacy Governance Framework
Incident Management	Implementation of an Incident Management Procedure that sets out how to manage data breaches with Personal Data
Policy & Procedure	A formally adopted and published a privacy policy that meets the minimum requirements set out in the VEON Group Privacy Policy as well in local data protection laws
Pre Screening of vendors	A process that ensures that a third party, prior to processing Personal Data for VEON (OpCo) will be assessed if it has implemented appropriate security controls to protect VEON (opCo) Personal Data

Privacy Assessments	A privacy assessment process to ensure that all privacy requirements (under data protection laws and the VEON Group Privacy Policy) will be met during the design phases of new solutions or processes that involve the processing of Personal Data.
Privacy Contracting	A process that ensures that a written contract containing legal as well as technical and organizational safeguards for the processing of (VEON Group) Personal Data is concluded with a third party, before Personal Data is transferred to that third party
Privacy transparency notices	Ensure that legally correct and complete privacy transparency notices are made available to the relevant individuals (for example to customers, employees or others) from whom Personal Data is or will be collected and processed. It also shall ensures that these notices are concise, easily accessible, and that clear and plain language is used so they are easy to understand
Records of Data Breaches	The Cyber Security department shall maintain records of data breaches with Personal Data. The record is kept at the central repository per VEON entity.
Regulatory Monitoring	(OpCo) Government Affairs and/or Regulatory will (on a frequent basis) monitor the introduction of new privacy regulations and timely assess potential cost impact
Reporting	Periodical reporting of status of local privacy compliance by OpCos (privacy leads or Privacy Officers) to the OpCo Business Risk Committee and the OpCo CEO.
Retention	A clear up-to-date data retention policy that determines what the applicable (minimum and maximum) retention periods are for Personal Data
Security measures for Personal Data	Implementation of appropriate technical and organizational measures to ensure a level of security appropriate to risks with the type of Personal Data
SPOC for the Privacy Authority	A formally appointed employee or department that is the point of contact for and maintains the relationship with the local Privacy/Data Protection Authority
Training	A privacy training and communication program that ensures employees are aware of requirements that follow from the VEON Entity privacy policy and local data protection laws. The program shall also include monitoring that all individuals have followed this privacy training

*As further detailed in the VEON Privacy Control Framework template

Annex III

Roles & Responsibilities

Owner of the VEON Group Privacy Policy (VEON Group CFO)
• Represents privacy policy-related activities within the Board of Directors of the VEON Group; • Develops and maintains the VEON Group Privacy Policy; • Has overall responsibility for the effectiveness of the implementation of the VEON Group Privacy Policy at HQ and the OpCos;

Owner of the OpCo Privacy Policy (OpCo CFO)

• Is accountable for OpCo compliance with this Policy and data protection laws;
• Oversees creation and implementation of OpCo privacy policies referencing this Policy and international standards and best practices ensuring compliance with data protection laws;
• Monitors OpCo compliance with this Policy and OpCo privacy policy and procedures;
• Reports the status of implementation of the Opco privacy policy to the OpCo Business Risk Committee;
• Reports to the Opco Business Risk Committee any matter that has the potential to violate, or is violating data protection laws, resulting in Material Liability, and any other matter involving personal and/or subscriber data that may be material to the reputation or operations of the OpCo or the Group, and, in any case, any Significant Matter. These reports shall include mitigating matters. Examples of Significant Matters are e.g.:
  • Sale of Personal Data: any transaction involving the grant of legal rights to a third party over personal and/or subscriber data collected by or through the operations of any VEON Group Entity;
  • Data breaches: any unauthorized access by a third party impacting the personal and/or subscriber data of more than (e.g. 500) individuals;
  • Cross border transfers: any cross border transfer with personal or subscriber data that may violate data protection laws;
  • Any project with Personal Data that is planned to cover a substantial part of the OpCo Customer base, and that has the potential to violate data protection laws.

OpCo Business Risk Committee
• Reviews the adoption of the OpCo privacy policy; • Performs oversight on the implementation of the OpCo privacy policy; • Reviews and provides guidance in relation to the by OpCos reported privacy compliance risks and proposed mitigation actions; • Reports to the OpCo Board any concerns related to by OpCos reported material privacy compliance risks and proposed mitigation actions.

On an operational level, compliance with this Policy is the responsibility of all VEON Group Personnel in particular those VEON Group Personnel whose role involves the handling, processing and use of Personal Data. As a general rule, responsibility for privacy compliance of IT platforms, applications and third parties that process Personal Data, lies with the business unit or function that owns these IT platforms and applications, or has contracted these third parties. They are through the relevant Business Owner (in that business unit or function) accountable for taking the required measures to ensure that their IT Platforms and applications are set up (or in case of third parties, instructed and bound through contracts) to comply with this Policy and data protection laws. For taking the right measures Business Owners can for advice and guidance go to the Primary Privacy Compliance roles, such as the EU Data Protection Officer (for VEON EU Entities) and OpCo Privacy Officers, as well as the Supporting Privacy Compliance Functions. The general roles of Business Owners as well as Primary and Supporting Privacy Compliance Functions set out below are recommended to be reflected in the HQ and OpCo privacy policies or procedures.

Business Owners

The business units and other functions in the VEON Group that processes, handle or use Personal Data are accountable for privacy compliance through the relevant Business Owner. This means that within these business units / functions, the Business Owner is responsible for:

- ensuring Personal Data is processed, handled or used in a manner compliant with its VEON entity's privacy policy and data protection laws;
- engaging Primary and Supporting Privacy Compliance functions for advice on the applicable privacy compliance requirements;

Primary Privacy Compliance Functions

OpCo Privacy Officer

Supports the OpCo CEO to meet its responsibilities under the VEON Group Privacy Policy;

- Oversees creation and implementation of privacy compliance policies, procedures and processes ensuring compliance with this Policy and Data Privacy Laws;
- Localizes the Privacy Control and Governance Frameworks (to ensure compliance with local data protection laws)
- Informs the relevant internal stakeholders of their responsibilities under the Privacy Control and Governance frameworks;
- Leads direction setting and decision taking with regard to all issues relating to Personal Data;
- Reports the status of implementation of the Group Privacy Policy, privacy risks and mitigating actions to OpCo Executive Committee and the local Business Risk Committee (BRC);
- Initiates and lead discussion with local regulatory authorities on privacy issues;
- Responsible for providing legal advice to all business lines and functions that process, handle or use personal information.

EU Data Protection Officer (as further clarified under GDPR article 38 and 39 and regulatory guidance)

VEON EU entities shall ensure that the EU Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the processing of personal data. The EU Data Protection Officer has the following responsibilities:

- Informs the VEON EU Entities about their responsibilities under GDPR;
- Monitors compliance with GDPR and the VEON HQ data protection program and policies;
- Ensures there is privacy training;
- Should be consulted on data protection impact assessments;
- Primary point of contact for the EU Data Protection Authorities;
- Prioritises with a risk-based approach;

Supporting Privacy Compliance Functions

Legal

The Legal department provides legal support and advice on data protection topics. Legal is responsible for:

- providing legal advice on data protection laws to all business lines and functions which process, handle or use Personal Data.
- providing legal input in relation to the development of privacy policies and procedures.

Regulatory/Government Affairs

Regulatory/Government affairs deals with (local) regulators and adherence to (local) laws and regulations including data protection laws. As such, Regulatory / Government Affairs is responsible for:

- monitoring new privacy laws and regulation as well as involvement in public consultation.
- initiating and leading discussion with local regulatory authorities on privacy issues.

Cyber Security

The Cyber Security department has a supporting and facilitating role relating to protecting Personal Data, and is responsible for:

- setting the information security strategy taking into account the business and the type of Personal Data that it processes, handles or uses.
- maintaining information security standards and policies for the relevant VEON entity.
- setting the company security strategy.
- threat detection and mitigation.
- providing direction and recommendations to the business on the technical and organisational measures required for their processing, handling or use of Personal Data.
- managing all Cyber Security incidents with Personal Data (including tracking of all remediation activities), with escalation to the Privacy Officer, EU Data Protection Officer and Legal as relevant.

Procurement

The Procurement department has a supporting role to the organization in engaging third parties. This means that Procurement is responsible for:

- making sure that third parties are assessed from security perspective, supported by Cyber Security.
- facilitating that written contracts containing legal as well as technical and organizational safeguards for the processing of (VEON Group) Personal Data are concluded with third parties, before Personal Data is transferred to these third parties.