



**Personal data
protection Policy**
European scope

summary

1. Aims	3
2. Scope	3
2.1 Entities, employees and data processors subjected to the Policy	3
2.2 Personal data and processing concerned	3
3. Management & Governance	4
3.1 At Group level	4
3.1.1 Group Governance	4
3.1.2 Group DPO	4
3.2 At BU level	4
4. Protection principles specified in the GDPR	5
4.1 Principle of accountability	5
4.2 Specific, explicit and legitimate purposes	5
4.3 Necessity, proportionality and minimization of personal data collected	5
4.4 Lawfulness of personal data processing	5
4.5 Transparency and the right to information	6
4.6 Right of access, rectification, restriction, erasure and objection	6
4.7 Classification, confidentiality levels and security of personal data	6
4.8 Integrating personal data protection into project management	6
4.9 Data protection Impact assessment	6
4.10 Relations with data processors	6
4.11 Transferring personal data outside the EU	7
4.12 Storage limitation	7
5. Operational implementation	7
5.1 Training and raising awareness	7
5.2 Provision of procedures and deliverables	7
5.3 Traceability of security incidents	7
5.4 Managing security incidents and breaches of personal data	8
5.5 Compliance reviews, controls, audits and fines	8

Compliance with fundamental rights and rules for protecting personal data is an integral part of the Group's ethical values.

The General Data Protection Regulation ("**GDPR**"),¹ which applies in all EU member states as from May 25, 2018, increases the rights of natural persons over their personal data and standardizes protection throughout the European Union.

The GDPR introduces the new principle of «accountability» of players in both the private and public sectors, which must be able to prove they have implemented the appropriate measures to ensure compliance with the protection rules.

These new requirements include appointing a Data Protection Officer ("**DPO**"), keeping a register to record compliance of personal data processing and implementing stricter security measures.

Failure to comply with these rules may result in heavy fines,² as well as harming the image of SUEZ.

Faced with these new challenges, the Group has decided to introduce a policy (the "**Policy**") aimed at ensuring the personal data of employees, clients and suppliers is protected, in compliance with its Ethics Charter.

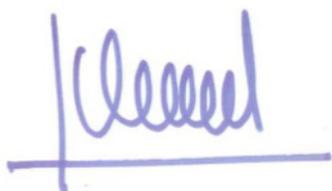
Protection of personal data is an asset for our digital transformation and helps to build long-term trust among our employees, clients and partners.

This is a highly important issue for the sustainable performance of our business.

The Group DPO, reporting to the Legal Department, is in charge of ensuring this Policy is applied on behalf of the General Secretary.

I would therefore like to ask all employees to become actively involved in ensuring it is correctly applied.

Jean-Louis CHAUSSADE
CEO



¹ EU Regulation 2016/679 of 04/27/2016 on the protection of natural persons as regards the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC, published in the Official Journal of the European Union on 05/04/2016.

² Fines can extend to 4% of the Group's global annual turnover of the previous year or €20 million, with the highest amount being applied.

1. Aims

This Policy, which has been approved by the Executive Committee, sets out the protection rules that SUEZ and its Group entities must implement for processing personal data³ in Europe.

The Policy includes all the principles designed to guarantee that the processing of personal data is lawful, fair and transparent. It sets out the rules of governance that stipulate the roles and responsibilities of those involved in personal data protection.

All employees, together with any person or entity outside the Group that processes⁴ personal data, are required to behave in compliance with the principles set out below.

Employees should contact their local DPO if they have any questions regarding the exercise of rights to access and correct personal data or for any questions or complaints about the processing of their own personal data, either by post or email at the address provided on their BU intranet.

For all questions on how to apply the Policy or any other issues, the Group DPO can be contacted at the following address: privacy@suez.com

2. Scope

2.1 - Entities, employees and data processors subjected to the Policy

This Policy applies to legal entities conducting business within the European Union ("EU"), irrespective of whether the data processing is performed within the EU.

This Policy applies to all employees, even occasional, and all data processors,⁵ as defined by the GDPR.

If any national regulation provides for stricter data protection standards than those specified in the GDPR, the national regulation prevails over the Policy.

The Group's legal entities subject to specific national regulations shall, if necessary, adopt supplementary documents of application in compliance with this Policy.

2.2 - Personal data and processing concerned

The Policy covers personal data on any paper or digital media that is hosted or processed, in particular:

- on any IT media, such as a server in a data center or in the cloud, a workstation or smart phone;
- via applications, databases or data warehouses;
- via portals exposed on the Internet or intranet;
- via smart objects or smart grids, and digitization projects.

The Policy applies to all processing involving the personal data of employees, clients, suppliers or partners that is collected, used or transferred by Group entities.

³ "Personal data" means any information relating to an identified or identifiable natural person, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

⁴ "Personal data processing" means any operation performed upon personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

⁵ "Data processor" means any legal or natural person that processes personal data on behalf of a Group entity.

3. Management & Governance

All employees must comply with the Policy.

The legal representatives of the Group's legal entities must ensure the Policy is distributed within their scope and in their teams. They are responsible for Policy implementation, assisted by the Group DPO and their network of local DPOs.

The Group DPO introduces a system of governance designed to set out the organizational measures specified in the GDPR and ensure the Policy is rolled out effectively. This governance is detailed in a specific guide on the governance of personal data (the "**Governance**").

3.1 - At Group level

3.1.1 - Group Governance

Policy implementation and compliance are supervised by the Data Protection Committee ("**DPC**"), which includes the Group DPO and the Group's Chief Information Security Officer ("**CISO**", reporting to the Information System Department) and is under the authority of the Group General Secretary.

Every year, the DPC draws up a summary report of its activities, which is then presented by the General Secretary to the SUEZ Ethics and Sustainable Development Committee, together with the proposed action plan for the following year. The DPC attributions and operational procedure are specified in the Governance.

3.1.2 - Group DPO

The Group DPO reports to the Group General Counsel, within the General Secretariat. The principal missions of the Group DPO are those provided for by article 39 of the GDPR and are listed in the Governance.

The main missions of the Group DPO include designing and supervising application of this Policy and coordinating the network of local DPOs.

3.2 - At BU level

Under the GDPR, each legal entity is responsible for its own personal data processing. It is therefore the responsibility of the legal representatives of these entities to ensure employees correctly apply the Policy in compliance with the GDPR.

Local DPOs are appointed under the responsibility of the legal representatives of entities and report at an operational level to the Group DPO.

Local DPOs define and control compliance with the GDPR and the Policy within their scope.

Local DPOs or, failing this, legal representatives provide assistance and advice for employees who ask questions or contact them with their concerns about personal data protection and ensure employees adopt practices that comply with the Policy, the GDPR and any applicable national regulations.

4. Protection principles specified in the GDPR

4.1 - Principle of accountability

Under the GDPR principle of accountability, each entity must:

- at all times, be able to document the way in which it protects personal data;
- introduce the appropriate technical and organizational measures to be able to prove that all personal data processing complies with the GDPR and any applicable national legislation.

In practice, this principle is implemented via the following measures:

- appointing a DPO, when this appointment is mandatory under the GDPR or applicable national regulations;
- keeping a record of data processing activities that includes the mapping of processing performed by the entities;
- conducting data protection impact assessments, in the cases rendered mandatory by the GDPR;
- protecting personal data from the start of any new project concerned (*privacy by design*);
- entities implementing appropriate procedures, in the case of risks generated by personal data processing related to their business activity.

4.2 - Specific, explicit and legitimate purposes

Personal data must be processed in a lawful, fair and transparent manner. It must be collected for specific, explicit and legitimate purposes and not be further processed in a manner that is incompatible with the original purposes.

Each entity must pay particular attention to processing special categories of personal data (sensitive data) that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data or data concerning the health, sex life or sexual orientation of a person.

Each entity may only process this type of personal data with the explicit consent of the data subject or in cases expressly authorized by national legislation and the GDPR.

4.3 - Necessity, proportionality and minimization of personal data collected

Personal data processed by entities must be accurate, necessary and restricted to the purposes for which it was collected.

4.4 - Lawfulness of personal data processing

Each entity must ensure the lawfulness of its personal data processing.

Personal data processing is lawful, as defined in the GDPR, when one of the following applies:

- compliance with a legal obligation to which the entity is subject;
- performance of a contract to which the data subject is party;
- legitimate interests pursued by the entity, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject;
- the data subject has given express consent for one or more specific purposes, in the cases provided for by the GDPR.

4.5 - Transparency and the right to information

Each entity must inform the subjects of personal data processing, using the wording required by the GDPR, via any information notice that ensures concise, transparent, intelligible and easily accessible communication.

When personal data is collected directly from the data subject, the information must be provided at the time the personal data is obtained.

In cases where the personal data is collected indirectly (e.g. by purchasing data files), data subjects must be informed without undue delay and within one month of collection and, in any event, no later than at the time of the first communication with the data subject or prior to any communication with a third party.

4.6 - Right of access, rectification, restriction, erasure and objection

Data subjects have rights of access, rectification and restriction over their personal data, together with rights to erase personal data (right to be forgotten), object to processing and the right to personal data portability, under the conditions set out in the GDPR.

They may exercise these rights at any time. The procedures for responding to the exercise of these rights are specified by local DPOs.

Each entity must ensure that the subjects of its personal data processing are effectively able to exercise their rights.

4.7 - Classification, confidentiality levels and security of personal data

Personal data is classified in accordance with the "SUEZ Information classification and confidentiality protection policy", available on the SUEZ intranet (Policies and Procedures section).

Documents containing current personal data are to be classified at "internal" level.

Documents containing special categories of personal data (sensitive data) are to be classified at "confidential" level.

In addition, each entity must take the necessary measures, based on the type of personal data, context and purpose of processing personal data, to guarantee a level of security in line with the identified risks.

The security level must guarantee the confidentiality, integrity and availability of personal data and limit any risk of destruction, loss, alteration, disclosure and unauthorized access to personal data.

Processed personal data must be protected in accordance with the Security Guidelines and the Information System Security Governance, which are both available on the SUEZ intranet (Policies and Procedures section).

4.8 - Integrating personal data protection into project management

Personal data protection must be integrated into project management and new services from the design stage onwards.

4.9 - Data protection Impact assessment

Each Group entity, acting as a data controller,⁶ must perform a data protection impact assessment prior to implementing any new personal data processing, when the criteria specified by the GDPR is met, in particular, in cases of wide-scale processing of special categories of personal data (sensitive data) or use of new technologies.

4.10 - Relations with data processors

Group entities that entrust the collection, use or processing of personal data to data processors, as defined by the GDPR, remain accountable for protecting this data. These entities must ensure the data processors provide sufficient guarantees with respect to this Policy and the GDPR. All contracts signed with data processors must set out its obligations, including security and confidentiality measures, in compliance with GDPR requirements.

⁶ "Data controller" means the natural or legal person, service or other body which, alone or jointly with others, determines the purposes and means of processing of personal data.

4.11 - Transferring personal data outside the EU

Personal data may only be transferred outside the EU in the following cases:

- when the destination country of the personal data is deemed to have adequate protection levels, based on the conditions set by the European Commission;
- when the recipient of the personal data can provide evidence of the appropriate guarantees enabling the effective exercise of the rights of data subjects, as defined in the GDPR;
- under the criteria for derogation stipulated in the GDPR: the explicit consent of the data subject, when transfer is necessary for the performance of a contract or for reasons of public interest, for the establishment, exercise or defense of legal claims or to protect the vital interests of the data subject.

4.12 - Storage limitation

It is the responsibility of each Group entity not to keep processed data beyond the period necessary for the purposes for which the data was processed, in compliance with applicable national legislation.

When personal data is no longer required for the purposes legitimizing its processing, it must be erased or rendered anonymous.

5. Operational implementation

The DPO network, Information System Departments, Information System Security Officers and the legal network shall assist the entities with implementing the Policy.

The following actions must be implemented to reach its objectives:

5.1 - Training and raising awareness

Local DPOs or, failing that, the legal representatives of entities, must ensure their employees have sufficient knowledge to fulfill their obligations under the GDPR and applicable regulations, according to the extent of their involvement in personal data processing.

Due to the importance of the issues surrounding personal data protection, all personnel concerned must take part in the awareness actions organized by the Group DPO and the local DPOs.

5.2 - Provision of procedures and deliverables

The Policy is to be rolled out using methodologies, procedures and awareness actions appropriate to the specific nature of applicable national regulations.

The Group regularly publishes thematic guides designed to disseminate best practices and enable the operational rollout of the objectives stipulated in the GDPR.

5.3 - Traceability of security incidents

In accordance with the Group's security rules, there is automated traceability of security incidents. Each entity can decide on the incidents to trace, based on the context, media (such as workstations, network equipment or servers), risks and requirements of each applicable legislation.

5.4 - Managing security incidents and breaches of personal data

Each Group entity must introduce a reporting procedure for security incidents and for managing personal data breaches, including for crisis management, in compliance with the GDPR and applicable regulations.

The Group DPO or local DPO, accordingly, and the legal representative of the entity, must be immediately informed of any personal data breach, as defined in the GDPR. If the reported breach could potentially seriously damage the rights and freedoms of the data subjects, the DPO must notify the relevant national data protection authorities (and, if necessary, the data subjects concerned) immediately (if possible, within 72 hours of becoming aware of the breach).

5.5 - Compliance reviews, controls, audits and fines

The technical and organizational measures to bring personal data processing into compliance are to be tested, analyzed and assessed to verify their effectiveness.

Internal controls are to be performed regularly to verify compliance with the GDPR, local regulations and the Policy. Data processors must provide the necessary information to prove they comply with legal obligations.

The performance of internal controls may, if necessary, be reviewed by the Internal Audit Department, supported by the Group IS Department if necessary.

The results of these controls may be communicated to the entity concerned, as well as to the Ethics and Sustainable Development Committee. They may also be made available to the relevant national data protection authorities, in compliance with the GDPR.

The corrective measures adopted in the event of any discrepancies identified during the compliance review shall be documented and regularly updated.

Each legal entity shall directly bear the cost of any fines that may result from failure to comply with the GDPR and applicable regulations with respect to its processing of personal data.

ready for the resource revolution  **SUEZ**