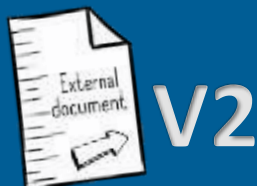


HOW WE COMMIT TO PRIVACY & DATA PROTECTION EVERY DAY

**Privacy & Data Protection
Guide of Good Conduct
ROQUETTE GROUP**



Legal & Compliance

Roquette's key compliance challenges

Under the leadership of the General Management, the compliance scope and its management within Roquette is a key part of the Group “Legal & Compliance” Department and known as the Compliance Office.

The Compliance Office owns the Roquette [Code of Conduct](#), its update and implementation.

It also covers the following three main areas:

- Financial security,
- Professional ethics and
- Privacy and Data Protection.

Therefore, a Compliance Program has been developed and is evolving to ensure that our business is legally and financially irreproachable.

What is the role of compliance?

The role of compliance is to instill **ethical values** and implement measures in accordance with **legal requirements, standards** and **good practices**.

Our Program facilitates the implementation of procedures ensuring compliance with the rules applicable to Roquette.

Our four values – **authenticity, excellence, forward-looking, well-being** – constitute the solid basis upon which we act **every day**.

Our Data Protection Strategy is People and Business Centric

The principles of Privacy & Data Protection are part of the standards set out in our Code of Conduct.

Ethics is increasingly talked about in terms of a key Group value – and data ethics is a key part of that.



Edito

The principles of Privacy and Data Protection are part of the standards set out in our Code of Conduct.

All employees, as well as third parties that Roquette has a relationship with, have a right to privacy. For this reason, Roquette is committed to protecting their personal data.

Personal data is information that allows directly or indirectly identifying a physical person (name, date of birth, social security number, photo, email address, computer IDs, etc.).

*The protection of
personal data is a
fundamental right
that ensures
privacy*

The protection of personal data guarantees each individual the right to control the collection, processing, use and distribution of this data.

Personal data must be used in a fair manner for a specific, explicit and legitimate purpose and must be kept only for the period needed to carry out processing.

In Europe, the processing of personal data has been defined by the General Data Protection Regulation (GDPR), which came into force the 25th May 2018.

Because legislation concerning privacy and personal data varies from country to country, and because Roquette is present internationally, the Group has adopted a Group Policy concerning personal data protection. This Policy applies to all Group employees worldwide.

This Guide explains Good Conduct to adopt in our daily activities to be compliant with Personal Data Protection Principles and our Policy's requirements.

Jennifer GODIN, Data Protection Officer



Déléguée à la protection
des données

Table of contents



Legal & Compliance		3
Edito from the Data Protection Officer		4
Purpose		6
Description		7
Responsibilities		8
Raising questions or concerns		9
Compliance with laws and regulations		10
Principles of data protection		12
Privacy Risk		14
Risks in the event of non-compliance		16
Our standards in our relationships with Data Subjects > p. 19		
• Culture of privacy	20	• Data Minimization 28
• Personal Data Processing	22	• Data Security 30
• Data Subjects' Rights	24	• Personal Information Classification 32
• Privacy Notice	26	• Data Retention 34
Our standards in our relationships with Affiliates and Subcontractors > p. 37		
• Qualification of processor & controller	38	• Data Transfer Agreement 42
• Data Protection Clauses	40	
Our standards in our relationships with our Network and Supervisory Authorities > p. 45		
• Data Protection Officer	46	• Documentation 56
• Data Protection Network & Stakeholders	48	• Privacy Impact Assessment 58
• Supervisory Authorities	50	• Privacy by Design & by Default 60
• Governance	52	• Data Breach Notification 62
• Accountability	54	• Review & Monitoring 64
Reference documents		66
Bibliography		67
Sources		68

Purpose

What is the Privacy & Data Protection Policy?

The Roquette Group has established a Privacy & Data Protection Policy (the “Policy”) in order to best address the issues of Privacy and Data Protection in line with its image, its interests and the applicable legislations and regulations regarding data protection.

This Policy defines the principles and requirements for the protection of personal information and indicates rules to be respected by all employees, managers, directors and third parties acting for Roquette in terms of Privacy and Data Protection.

The principles and rules of this Personal Data Protection Policy are detailed in a documentary platform with three levels:

- Management commitment: Code of Conduct
- Internal rules: Personal Data Protection Manual and Directives.
- Data Protection Management System (DPMS) Documentation: Procedures, Guidelines, Methodologies, Learning, etc.

All documentation complies with the legal and regulatory requirements for data protection.

What is the Privacy & Data Protection Guide of Good Conduct?

The Privacy & Data Protection Guide (the “Guide”) may help us to implement and comply with our privacy & data protection policy.

It presents - in a simplified manner - rules and best practices that comply with our Group directives and the requirements of the laws and regulations applicable to us in terms of data protection.

It is divided into themes inspired by the Code of Conduct, of which "Privacy & Data Protection" is one of the compliance topics.

Description

To whom does the Privacy & Data Protection Guide of Good Conduct apply?

The Policy and the Guide are common ground for all entities worldwide. They apply to:

- All employees, directors and managers (“the Employees”)
- Any third parties acting for Roquette, as:
 - Contractors, including consultants, freelancers and temporary staff
 - Trainees
 - Seconded staff from a non-Roquette entity
 - Casual workers
 - Other representatives
 - And any third party employed or paid by Roquette.

Where can we find the Privacy & Data Protection Guide of Good Conduct?

All Employees and third parties acting for Roquette must understand and respect the Privacy & Data Protection principles contained in our Documentation and especially in the present Guide.

The Guide is close at hand on:

<https://www.roquette.com/data-protection>.

This Guide is broadcasted as part of a dedicated communication, accompanied by toolkit with e-learning courses on Privacy & Data Protection Principles (defined by international standards and specifics requirements of the GDPR).



Responsibilities

Who is responsible for the implementation of the operational Principles?

Data privacy is relevant to – and the responsibility of – everyone in our organization.

We all have a responsibility to respect the operational Principles described in the DPMS Documentation provided by the Compliance Office Team and the Data Protection Network. This Guide supports this implementation and increases our level of compliance.

How can we make sure that we take the right decision?

The Guide is designed to help us deal with most of the situations in our working life that might pose privacy questions. However, it cannot foresee every situation we may face in the exercise of our professional activities.

If we have any doubt, at any time, about what attitude to adopt, we must use good judgement and ask ourselves the following questions:

- Does this comply with the law?
- Does this reflect well on me and on the company?
- Would I tell a friend, family or colleague about this?
- Would I feel comfortable if this were made public?

If the answer to any of these questions is 'No', we should not proceed. If we are in any doubt, we should speak to the Group Data Protection Officer or other relevant contact (see contact information in the section 'Raising questions or concerns').

What happens if we do not comply with the Privacy & Data Protection Principles?

Failure to respect the Principles can have an adverse effect on the company. The consequences can be very serious, both for the company and for the involved individuals (disciplinary sanctions, fine, imprisonment, damaged reputation, etc.).

All reports of actual or suspected Principles violations will be taken seriously. We will investigate promptly, fairly and in accordance with legal requirements.

Depending on the nature of the Data Breach, disciplinary measures may be imposed, pursuant to local laws and company regulations.

All employees are required to cooperate fully with any investigation. Roquette will protect the confidentiality of anyone involved.

Raising questions or concerns

Employees, third parties acting for Roquette, and other stakeholders are encouraged to raise questions or concerns that will help Roquette prevent and reduce any harm to the company.

What kind of issues can be raised?

Any questions, and any potential or actual violation of the Privacy & Data Protection Principles, company regulations or applicable laws, can be raised.

Whom should we contact?

In case of Data Breach please contact the Data Protection Officer at dpo@Roquette.com and/or report an incident by our [Privacy Alert webform](#).

If you need to report a potential compliance violation you can get in touch with your usual point of contact or report a problem through the [Speakup](#)© device. All alerts received through this device are dealt with confidentially, respecting relevant laws and regulations.



Roquette will not tolerate any form of reprisal or retaliation against an employee or a third party who reports, in good faith, a potential or actual compliance violation of the Privacy & Data Protection Principles or applicable laws.

Therefore, if the issuer of a professional alert must identify himself/herself, his/her identity must be processed confidentially by the organization, in order to avoid the risk of reprisals, discrimination or disciplinary measures being taken against him/her for having denounced the facts.



Compliance with laws and regulations

Every one of us, in each entity of the Group, is expected to comply with the laws and regulations in force regarding Data Protection.

In cases where local regulations are stricter than our Policy and Guide, the former will prevail.

Otherwise (absence of local legislation or less restrictive legislation), our internal good practices will prevail to the extent permitted by law.

We consider that:

- We must implement as quickly as possible all new local and applicable regulations.
- Each of us must be aware that any breach of laws and regulations may be liable to civil and/or criminal sanctions, both for the individual involved and for the company.
- The protection of natural persons in relation to the processing of personal data is a fundamental right.
- The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data.
- The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.

Which country has adopted a specific data protection legislation or has a Data Protection Authority?

To get an overview, consult this map:

<https://www.cnil.fr/en/data-protection-around-the-world>.



Our responsibilities:

- Under all circumstances, we must comply with all applicable laws and regulations regarding Data Protection in the countries of the Data Subjects and all rules in force at each of the company's locations.
- As part of our professional activities, we should report any behavior which we consider to be against applicable laws and regulations regarding Data Protection (e.g.: GDPR) to our Data Protection Officer at dpo@Roquette.com and the confidential Roquette alert device: [Speakup©](#).
- We must put in place personal data protection measures that are appropriate and proportionate to the context while facilitating compliance with other laws and regulations. Conversely, our actions to comply with the laws and regulations applicable to the Group must comply with the rules and good practices for the protection of personal data (example: in the Anti-Bribery and Corruption compliance program, we must ensure the protection of the whistleblower through measures of confidentiality and protection of his personal data).

ARE YOU SUBJECT TO THE GENERAL DATA PROTECTION REGULATION (GDPR)?

You come within the scope of the GDPR as a **processor** ⁽¹⁾ or a **controller** ⁽²⁾:

- if you are established in the EU or;
- when you are not established in the EU, if: your "processing activities are related to
 - the offering of goods or services to data subjects in the EU;
 - or the monitoring of their behaviour as far as their behaviour takes place within the EU" .

Official text: Article 3 of the GDPR on the Territorial Scope

(1) & (2): See definitions on page [38](#).



Principles of Data Protection

Personal data must be:

- secure.
- accurate and up to date.
- processed fairly and lawfully.
- processed for limited purposes.
- adequate, relevant and not excessive.
- kept for a limited and determined period of time.
- processed in accordance with the data subject's rights.
- protected by appropriate legal measures if transferred to other countries.



Your Rights:

In accordance with the applicable legislation and regulations, you have the right to access, rectify and oppose the processing of your data for legitimate reasons, as well as the right to erasure for legitimate reasons, the right to data portability, and the right to limit the processing of your data.

To exercise these rights, please fill in the form available at: [Roquette.com/Data Protection](https://Roquette.com/Data%20Protection).

For any requests, please contact the Data Protection Officer (dpo@Roquette.com).

Our responsibilities:

We must:

- Follow local legislation and the Group Policy rules concerning Personal Data Protection.
- Notify the Data Protection Officer of any new processing or changes.
- Not collect, use, disclose or store data of a personal nature unless it is for specific, legitimate and necessary purposes.
- Ensure that individuals have been informed that their data are being collected.
- Protect these data during collection, processing, use, communication, storage or transfer.
- Ensure the safety and confidentiality of processed data.
- Keep data only for the time needed for processing and follow the applicable laws.
- Contact the Data Protection Officer in the event of a security incident involving personal data.

We train our employees and improve our internal processes.

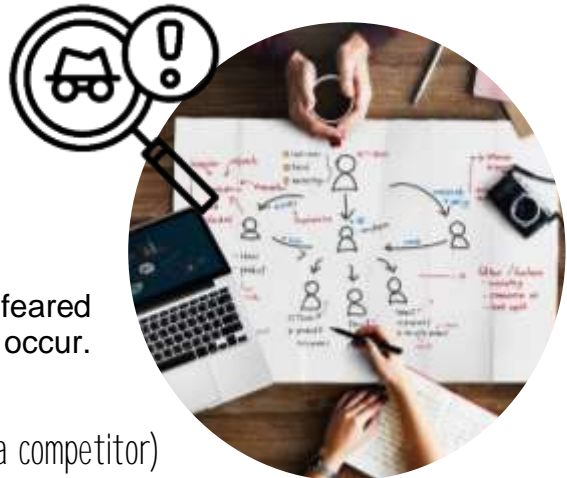


Privacy risk

What is a privacy risk?

A risk is a hypothetical scenario that describes a feared event and all the threats that would allow this to occur. More specifically, it describes:

- how risk sources (e.g.: an employee bribed by a competitor)
- could exploit the vulnerabilities of supporting assets (e.g.: the file management system that allows the manipulation of data)
- in a context of threats (e.g.: misuse by sending emails)
- and allow feared events to occur (e.g.: illegitimate access to personal data)
- on personal data (e.g.: customer file)
- thus generating impacts on the privacy of data subjects (e.g.: unwanted solicitations, feelings of invasion of privacy, personal or professional problems).



Effect of uncertainty on privacy

Severity represents the magnitude of a risk. It is primarily estimated in terms of the extent of potential impacts (**physical, material, moral**) on data subjects, taking account of existing, planned or additional controls.

Example:

The most important risk presented by the professional alert system for the whistleblower: the risk of reprisals, discrimination or disciplinary measures being taken against him/her for having denounced the facts.

We consider that:

Individuals' rights apply in full irrespective of the level of risk in the processing.

However, we will be required to modulate our data protection compliance according to the level of risk that our personal data processing operations pose to the fundamental rights and freedoms of individuals.

The GDPR gives further impetus to this practice. Consequently, processing operations which raise lower risks to the fundamental rights and freedoms of individuals may generally result in fewer compliance obligations, whilst “high-risk” processing operations will raise additional compliance obligations, such as Data Protection Impact Assessments (DPIA) ⁽¹⁾

Our responsibilities:

Risk assessment is fundamental. Under the GDPR, consideration of risk underlies organizational accountability and all data processing.

We have to conduct risk assessments as part of DPIAs for high-risk processing, as well as in connection with many other GDPR requirements, including Data Security, Security and Data Breach notifications, Privacy by Design, legitimate interest, purpose limitation and fair processing.

(1): See definition on page [58](#).



Risks in the event of non-compliance

Legal and natural persons that do not comply with the law and regulation on data protection (e.g. GDPR) risk sanctions and costs, in the form of:

Criminal sanctions:

- Imprisonment.
- Fine for legal entities.

Civil sanctions:

- Civil damages.

Administrative sanctions:

- Formal notice.
- Warning.
- Injunction.
- Temporary or definitive limitation of processing.
- Withdrawal of a certification or injunction to withdraw a certification.
- Suspension of data transfers.
- Injunction to cease the processing or withdrawal of the authorization.
- Publicity of the sanctions imposed.
- Sanctions without prior formal notice (urgency criterion).
- Depending on the violation, an administrative fine.

Significant costs:

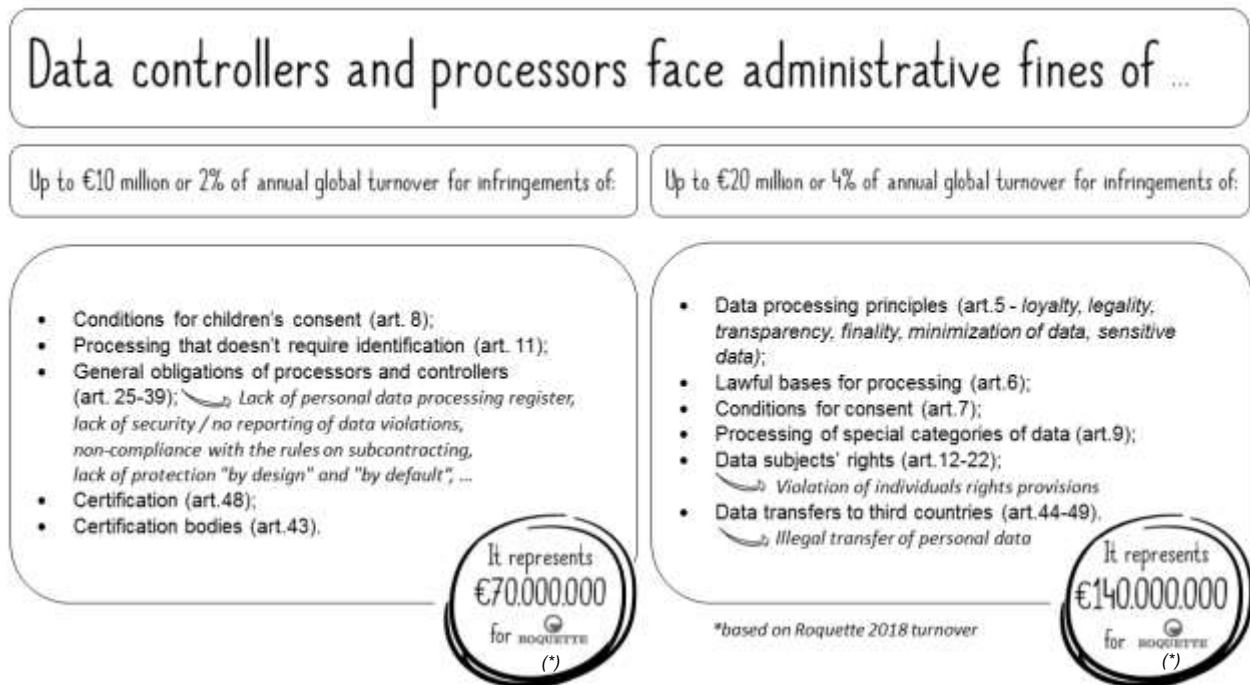
- Loss of revenue resulting from damage to their reputation.



What is the maximum administrative fine under the GDPR?

Fines are discretionary rather than mandatory. They must be imposed on a case-by-case basis and should be “effective, proportionate and dissuasive”.

The fines are based on the specific articles of the Regulation that the organization has breached.



What can be the criminal sanctions?

Few examples of French laws:

- The act of collecting personal data by fraudulent, unfair or unlawful means shall be punishable by five years' imprisonment and a fine of €300,000 (Penal code Art. 226-18).
- In order to guarantee a real right and protection of the whistleblower, the anticorruption law (Sapin II) severely punishes any obstacle to an alert. Confidentiality surrounding the alert is an essential element of regulation. Thus, the disclosure of confidential elements of the alert (identity of the whistleblower, of the defendant, information provided in support of the alert), except with regard to the judicial authority, is punishable by two years' imprisonment and a fine of €30,000.





1 Our standards in RELATIONSHIPS WITH DATA SUBJECTS

Culture of Privacy

Data protection is a set of laws, regulations and best practice directing the collection and use of personal data about individuals.

Personal data means any information relating to an identified or identifiable natural person.

Data privacy refers to the handling of personal data.

Who is concerned?

Data privacy is relevant to – and the responsibility of – everyone in our organization.

Why is it important?

Mishandled data can have serious repercussions for organizations, their employees and their customers.

Privacy breaches can lead to limitless financial penalties, bad press, damaged reputation, loss of trust from customers, loss of business and for employees, claim and perhaps plaint in case of privacy breaches on their own personal data, the prospect of disciplinary action in other cases. It is in all of our interest to handle data appropriately.

We consider that:

- All employees of Roquette must be made aware of their roles and responsibilities regarding the protection of personal data. The raising of awareness aims to reinforce the culture of respect for the privacy and protection of personal data within Roquette.
- Training of employees on the implementation of the personal data protection policy must be delivered.

[DIDPGRO01EN – Rule 1]

[DIDPGRO01EN – Rule 2]



THINK PRIVACY

It is our responsibility!

We need customer and employee personal data to run our business successfully.

We are trusted to look after this essential information.

Each and every employee has a responsibility to comply with the appropriate Data Protection laws.

It is our reputation!

Reputations are hard won and easily lost.

Handling our customer and employee data with care and respect is critical to protect our reputation.

YOU are our best defense against reputational damage.

It is about respect!

The choices our customers and employees make about how their personal data is used must be respected if we are to maintain the trust they place in us.

It is in your hands!

We are all responsible for ensuring that customer and employee personal data is kept secure and confidential.

Extra care must be taken with any information that needs to be sent or taken off-site.

We train our employees and improve our internal processes.

- Code of conduct – Privacy and Data Protection - p. 42 – 43.
- For new comers: Several information and e-Learning on Data Protection are delivered during the Global Onboarding.
- For employees: Learning are uploaded on Learning platform.
- For Data Protection Coordinators: Documentation is shared on our Community “Data Protection Network”.
- For all: More information are available on internal portal > Data Protection.



Personal Data Processing

Personal Data Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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.

A Data Protection (and GDPR) requirement you will need to be aware of is that you need to have a “lawful basis” for collecting any personal data.

Depending on the local legislation, there may be different legal bases.

What is my “lawful basis” for processing personal data?

You need to be able to clearly answer the question:

“How did you get my [piece of data] and why are you allowed to have it?”

More specifically, it means that you need to comply with at least one of the six lawful basis for processing data. Under GDPR, you cannot process any data unless:



1. Consent
2. Contract
3. Legal obligation
4. Vital interests
5. Public task
6. Legitimate interest



Lawfulness, fairness and transparency

Our responsibilities:

We have to apply rules to ensure the lawful processing of personal data.

Rules	Reference OneDoc	Reference GDPR
<ul style="list-style-type: none">• Act with lawfulness, fairness and transparency when collecting data	DIDPGR002EN Rule 1	Art. 5 1. a)
<ul style="list-style-type: none">• Demonstrate that the consent of the persons concerned is respected (when required)	DIDPGR002EN Rule 2	Art. 7
<ul style="list-style-type: none">• Respect the purposes determined during the collection of the data	DIDPGR002EN Rule 3	Art. 5 1. b)
<ul style="list-style-type: none">• Limit information collected on paper or digital forms to what is strictly necessary	DIDPGR002EN Rule 4	Art. 5 1. c)
<ul style="list-style-type: none">• Limit data retention to what is strictly necessary	DIDPGR002EN Rule 5	Art. 5 1. e)
<ul style="list-style-type: none">• Take measures to transfer personal data to third countries or international organizations	DIDPGR002EN Rule 6	Art. 44 to 50

We train our employees and improve our internal processes.



Data Subjects 'Rights'

Data subject means a natural person who can be identified, directly or indirectly, 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 the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

What is a 'data subject'?

This is the technical term for the individual whom particular personal data is about.

What is a subject access request?

One of the main rights which the Data Protection laws in force give to individuals is the right of access to their personal information.

An individual can send you a 'subject access request' requiring you to tell him/her about the personal information you hold about him/her, and to provide him/her with a copy of that information. In most cases you must respond to a valid subject access request within 30 (*) calendar days of receiving it.

(*): This period may vary depending on the applicable law or the nature of the data processing operation.

What are the other Data Subjects 'rights'?



Our responsibilities:

We have to apply rules to ensure the rights of data subjects.

Rules	Reference OneDoc	Reference GDPR
<ul style="list-style-type: none">• Make sure the legal notices comply with the obligations	DIDPGR006EN Rule 1	Art. 12
<ul style="list-style-type: none">• Permit data subjects to exercise their access rights	DIDPGR006EN Rule 2	Art. 15
<ul style="list-style-type: none">• Permit data subjects to exercise their right to rectification	DIDPGR006EN Rule 3	Art. 16
<ul style="list-style-type: none">• Permit data subjects to exercise their right to data portability	DIDPGR006EN Rule 4	Art. 20
<ul style="list-style-type: none">• Permit data subjects to exercise their right to erasure ('right to be forgotten')	DIDPGR006EN Rule 5	Art. 17
<ul style="list-style-type: none">• Permit data subjects to exercise their right to restriction of processing	DIDPGR006EN Rule 6	Art. 18
<ul style="list-style-type: none">• Notify rectification or erasure of personal data or restriction of processing	DIDPGR006EN Rule 7	Art. 19
<ul style="list-style-type: none">• Control automated individual decision-making, including profiling	DIDPGR006EN Rule 8	Art. 22

We train our employees and improve our internal processes.



Privacy Notice

The right to be informed if personal data is being used

We must inform you as employees, and all third parties that Roquette has a relationship with, if we are using your/their personal data.

We should provide detailed information on the following:

- Why Roquette is using your/their data.
- What type/types of data Roquette is using.
- How long your/their data will be kept.
- Your/their information rights.
- Where the data is from.
- Information if Roquette is going to transfer your/their data to third parties, including your/their names and the reasons for the transfer.
- Information if it is going to transfer the data in other jurisdiction, including the country involved and what will be done with the data.
- If Roquette is using the data in profiling (a type of automated processing where their personal data is used to analyze or predict things such as your performance at work, economic situation, health).
- How to contact the DPO.
- If concerned, your/their right to complain to the Supervisory Authority.



This is called **Privacy Information** or **Privacy Notice**.

We should give you/them privacy information at the time Roquette collects your/their data. If Roquette obtains your/their data from another source, it should provide privacy information. It may do so in the form of a privacy notice.

This is called **the right to be informed**.

Rules

	Reference OneDoc	Reference GDPR
<ul style="list-style-type: none"> Make sure the legal notices comply with the obligations 	DIDPGRO06EN Rule 1	Art. 12

Example:

- Privacy information on Roquette Website available on:
<https://www.roquette.com/privacy-notice-website> .

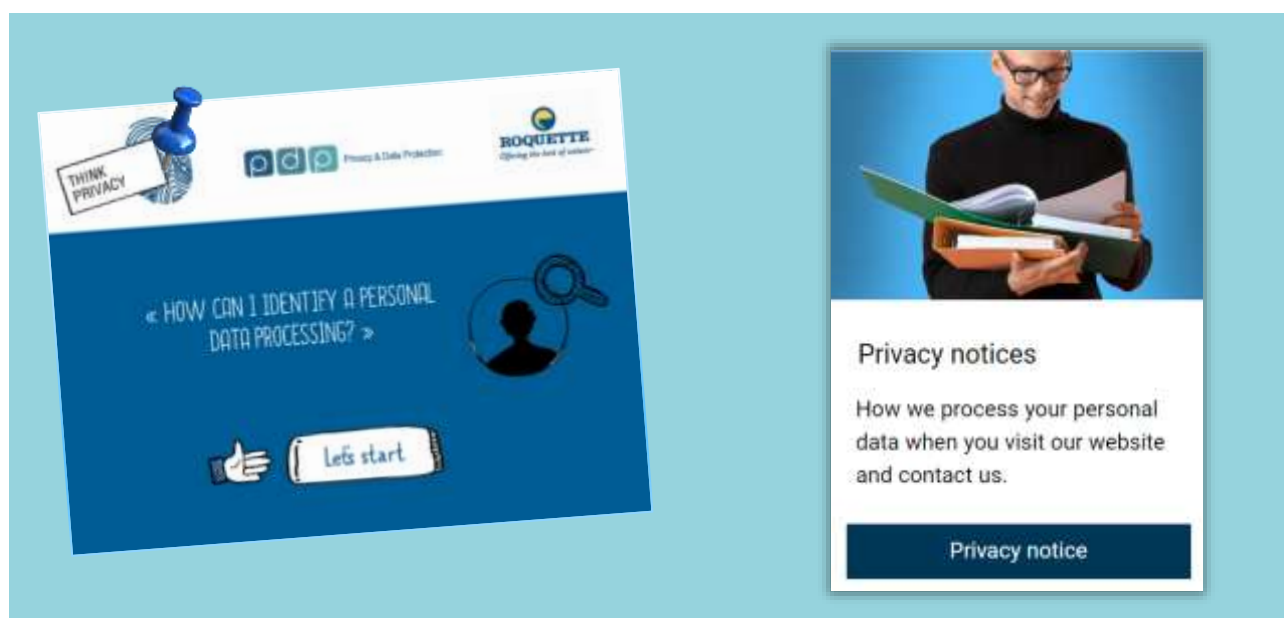
When can Roquette not inform you/them of its activities?

Generally, we must give you/them privacy information, but in some circumstances we don't have to. These include where:

- you/they already have the privacy information and nothing has changed,
- giving you the privacy information is impossible or would require "disproportionate effort", or
- giving you the privacy information would make it impossible to use your data or seriously damage the reasons for its use.

Note: Where provisional measures are necessary to avoid the concealment or destruction of evidence, such information may be issued after the adoption of the provisional measures.

We train our employees and improve our internal processes.



Data Minimization

What is the data minimization principle?

GDPR - Article 5(1)(c) says:

“1. Personal data shall be:

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization)”

Paper or digital forms designed by the Global functions to collect personal data should contain only information fields strictly necessary for the purpose of the processing in order to avoid collecting data that are not justified by the processing.



Our responsibilities:

We must ensure the personal data you are processing is:

- adequate – sufficient to properly fulfil your stated purpose;
- relevant – has a rational link to that purpose; and
- limited to what is necessary – you do not hold more than you need for that purpose.

Rules

	Reference OneDoc	Reference GDPR
<ul style="list-style-type: none">• Limit information collected on paper or digital forms to what is strictly necessary.	DIDPGROOZEN Rule 4	Art. 5 1. c)

Checklist:

- ☑ We only collect personal data we actually need for our specified purposes.
- ☑ We have sufficient personal data to properly fulfil those purposes.
- ☑ We periodically review the data we hold, and delete anything we don't need.
- ☑ We should identify the minimum amount of personal data we need to fulfil our purpose. We should hold that much information, but no more.

The accountability principle means that you need to be able to demonstrate that you have appropriate processes to ensure that you only collect and hold the personal data you need.

Also bear in mind that the GDPR says individuals have the right to complete any incomplete data which is inadequate for your purpose, under the right to rectification. They also have right to get you to delete any data that is not necessary for your purpose, under the right to erasure (right to be forgotten).

We train our employees and improve our internal processes.



Data Security

Cyber security is a transversal activity whose implementation ensures that data can be shared and used with a suitable and guaranteed level of protection of related information and assets:

- **Confidentiality**: ensures that information is kept confidential and not disclosed to inappropriate persons or entities,
- **Integrity**: safeguards the accuracy and completeness of information and processing methods,
- **Availability**: ensures that authorized users have always access to information, applications and services when needed,
- **Traceability**: refers to the capability to keep relevant tracks and, when required, proofs of what was done on our systems. Traceability also covers legal objectives such as non-repudiation or accountability.

Personal Information assets include:

- Paper documents (texts, maps, pictures...),
- Digital information in office environment,
- Digital information in mobile environment,
- Professional know-how and skills (owned by individuals or orally shared),
- Physical items (such as samples, strains, models...).



[DSUG006EN] Management of the Cyber Security Directive

Pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Anonymization is the process by which Personal Data is irreversibly altered in such a way that a Data Subject can no longer be identified directly or indirectly, either by the data **controller** ⁽¹⁾ alone or in collaboration with any other party.

Encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.

(1): See definition on page [38](#).

We consider that:

In order to maintain security and to prevent processing in infringement of data protection laws & regulations, Roquette and our subcontractors should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as **encryption** or **pseudonymization**.

Our responsibilities:

We need to implement security measures when we are handling any type of personal data, but what we put in place depends on our particular circumstances. We need to ensure the confidentiality, integrity and availability of the systems and services we use to process personal data.

Amongst other things, this may include information security policies, access controls, security monitoring, and recovery plans.

Appropriate security measures must be taken throughout the personal data life cycle and by all stakeholders.

Rules	Reference OneDoc	Reference GDPR
<ul style="list-style-type: none">Applying and reviewing the security measures defined in the security policy and directives	DIDPGR007EN Rule 1	Art.32
<ul style="list-style-type: none">Integration of information security and data protection review into projects.	DIDPGR007EN Rule 2	Art.32
<ul style="list-style-type: none">Security, Privacy & Data protection by design and by default	DIDPGR007EN Rule 3	Art.25
<ul style="list-style-type: none">Integration of information security and data protection clauses with subcontractors	DIDPGR007EN Rule 4	Art.32

We train our employees and improve our internal processes.



Personal Information Classification

The processing of sensitive personal data and some special categories of personal data is prohibited except in specific cases.

These processing require protective measures in terms of:

Marking, Access, Transmission, Transport, Copy and printing, Storage and archiving, Destruction.



Classification indicates the protection adapted to the sensitivity of the information or the document.

The decision to classify any information or a document is mandatory and must take place at the earliest stage.

[DISUGR001EN] Directive on Information Protection

Personal data types	Personal data categories
Common personal data	Civil status, identity, identification data
	Personal life (living habits, marital status, etc. –excluding sensitive or dangerous data)
	Professional life (résumé, education and professional training, awards, etc.)
	Economic and financial information (income, financial situation, tax situation, etc.)
	Connection data (IP addresses, event logs, etc.)
	Location data (travels, GPS data, GSM data, etc.)
Personal data perceived as sensitive	Social security number
	Biometric data
	Bank data
Sensitive personal data in the meaning of [DP-Act]	Philosophical, political, religious and trade-union views, sex life, health data, racial or ethnic origin, data concerning health or sex life
	Offenses, convictions, security measures

Our responsibilities:

Rules	Reference OneDoc	Reference GDPR
<ul style="list-style-type: none"> • Respect the legal framework for the processing of sensitive data 	DIDPGR004EN Rule 1	Art.9
<ul style="list-style-type: none"> • Prohibit the processing of data on criminal convictions and offenses 	DIDPGR004EN Rule 2	Art.10
<ul style="list-style-type: none"> • Limit access to health data only to authorized professionals 	DIDPGR004EN Rule 3	Art.9
<ul style="list-style-type: none"> • Prohibit the use of the national identification number as a unique identifier 	DIDPGR004EN Rule 4	Art.87
<ul style="list-style-type: none"> • Restrict access to and use of banking data 	DIDPGR004EN Rule 5	Art.9
<ul style="list-style-type: none"> • Restrict access to sensitive data to authorized persons only 	DIDPGR004EN Rule 6	Art.9
<ul style="list-style-type: none"> • Conduct impact assessments on the privacy of data subjects involved in sensitive data processing 	DIDPGR004EN Rule 7	Art.35
<ul style="list-style-type: none"> • Limit use of comment field to general information 	DIDPGR004EN Rule 8	Best practice

Some practical tips...

Examples of protective measures to be taken for every category of classified information assets (paper, digital, know how, physical).



Data Retention

The growing need to dematerialize operations and information exchange between the Group, our customers and business partners, as well as legal and regulatory requirements, have subjected Roquette to a number of obligations in terms of the length of the data retention period and records management policies.

Based on our activities, Roquette acquires and processes a large amount of sensitive data related to our strategy, financial results, commercial development or commitments, **as well as personal data related to our clients, business partners and staff members.**

Information sent or received by Roquette in connection with our activities must be kept for a minimum retention period, even though nothing prevents the company from keeping them in the archives for longer periods, **except in the event that they contain personal information.**



This time limit, during which the administrative and competent authorities can conduct post-inspections, varies based on the nature of the information to keep and the relevant legal requirements.

Infinite or indeterminate storage times are prohibited.

GDPR Art. 5 1. E)

‘storage limitation’

Personal data shall be 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.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required in order to safeguard the rights and freedoms of the data subject.

Our responsibilities:

- Roquette as data controller must define specific and adequate storage times for each category of personal data collected and processed.
- Prior to the implementation of personal data processing, the project owner with the assistance of a Data Protection coordinator must specify in our register, the duration of data retention.
- We must keep personal data only for the time needed for processing and follow the applicable laws.

Rules

	Reference OneDoc	Reference GDPR
<ul style="list-style-type: none">• Limit data retention to what is strictly necessary	DIDPGR002EN Rule 4	Art. 5 1. E)

In this respect, the Global Functions, GBUs and areas are committed to complying with the Company Information Retention rules and maintaining the associated procedures in operational condition.

Example:

At the end of a recruitment process, we must delete information on unsuccessful candidates, unless they agree to remain in our "pool" for a limited period (2 years).

We train our employees and improve our internal processes.





2 Our standards in RELATIONSHIPS WITH AFFILIATES and SUBCONTRACTORS

Qualification of processor and controller

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Joint Controller means two or more controllers who jointly determine the purposes and means of processing. However, regardless of those arrangements, each controller remains responsible for complying with all the obligations of controllers under the GDPR.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Who is a processor in the meaning of the General Data Protection Regulation?

(Article 4 of the GDPR – Definitions).

A very wide variety of service providers have the capacity of processor in the legal sense of the term. Processors' activities can concern a very specific task (sub-contracting of mail delivery) or be more general and wide-ranging (management of the whole of a service on behalf of another organization, such as managing the pay of employees for example).



The following are particularly concerned by the GDPR:

- IT service providers (hosting, maintenance, etc.), software integrators, cybersecurity companies or IT consulting companies (formerly known as IT engineering service companies) that have access to data,
- marketing or communication agencies which process personal data on behalf of clients, and
- more generally, any organization providing a service which entails personal data processing on behalf of another organization,
- a public authority or association may also be considered as such.

Insofar as they do not have access to or process personal data, software publishers and manufacturers of equipment (such as clocking terminals, biometric equipment or medical equipment) are not concerned.

Example of qualification of processor and controller:

Company A provides a marketing letter delivery service using the client data files of companies B and C.

Company A is a processor for companies B and C insofar as it processes the necessary client data for sending the letters on behalf of and on instructions from companies B and C.

Companies B and C are their clients' management controllers, including as regards the delivery of marketing letters.

Company A is also the controller regarding the management of staff it employs, and the management of its clients which include companies B and C.

Official text

- Article 4 of the GDPR for the definitions of controller and processor
- Article 28.10 of the GDPR on the notion of controller

We train our employees and improve our internal processes.



Data protection clauses

When is a contract needed and why is it important?

Whenever, as a controller, we use a processor to process personal data on our behalf, a written contract needs to be in place between the parties.

The contract is important so that both parties understand our responsibilities and liabilities.



Contracts with specific data protection clauses and/or data protection agreement between Roquette, as controller, and its processors ensure we both understand our obligations, responsibilities and liabilities. Contracts also help us comply with the GDPR, and assist us in demonstrating to individuals and regulators our compliance as required by the accountability principle.

What responsibilities and liabilities do we have as controller when using a processor?

We must only use processors that can give sufficient guarantees they will implement appropriate technical and organizational measures to ensure their processing will meet GDPR requirements and protect data subjects' rights.

As Controller, we are primarily responsible for overall compliance with the GDPR and other data privacy laws in force, and for demonstrating that compliance. If this isn't achieved, we may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

What is new under the GDPR?

The GDPR makes written contracts between controllers and processors a requirement, rather than just a way of demonstrating compliance with data protection principle (appropriate security measures) under Data Protection laws in force.

These contracts must now include specific minimum terms. These terms are designed to ensure that processing carried out by a processor meets all the GDPR requirements, not just those related to keeping personal data secure.

Rule	Reference OneDoc	Reference GDPR
<ul style="list-style-type: none"> Integration of information security and data protection clauses with subcontractors. 	DIDPGR007EN Rule 4	Art. 32
<ul style="list-style-type: none"> Contractors security 	DSUG016EN	

What needs to be included in the contract?

Contracts must set out:

- ☑ the subject matter and duration of the processing;
- ☑ the nature and purpose of the processing;
- ☑ the type of personal data and categories of data subject; and
- ☑ the controller's obligations and rights.

Contracts must also include specific terms or clauses regarding:

- ☑ processing only on the controller's documented instructions;
- ☑ the duty of confidence;
- ☑ appropriate security measures;
- ☑ using sub-processors;
- ☑ data subjects' rights;
- ☑ assisting the controller;
- ☑ end-of-contract provisions; and
- ☑ audits and inspections.

We train our employees and improve our internal processes.

- [Guide](#) on Data Protection for subcontracts compliant with the GDPR.
- Data Processing Agreement template available in our Privacy Management System: OneTrust@Roquette> Vendor Risk Management module.



Data transfer agreement

A **Data Transfer** is any communication, copy or transit of personal data (such as hosting servers, sending attachments by e-mail, remote access tools, screen sharing, etc.) intended for processing in other countries that do not have the same applicable personal data protection laws.

We are more connected than ever. For Roquette operating on a global scale, the international transfer of data is an essential element of daily business operations. Roquette, for example, store employee personal data in a cloud service hosted abroad and share employee & customer personal data between its subsidiaries established around the world.

How will the GDPR and others data protection laws in force affect such international data transfers?



Our responsibilities:

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if:

- The local law permits it and/or the supervisory authority has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection or has given its authorization, and/or
- A legal measure is taken (e.g.: Binding Corporate Rules or standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, etc.).

Rule	Reference OneDoc	Reference GDPR
<ul style="list-style-type: none">• Take measures to transfer personal data to third countries or international organizations	DIDPGR002EN Rule 5	Art. 44 to 50

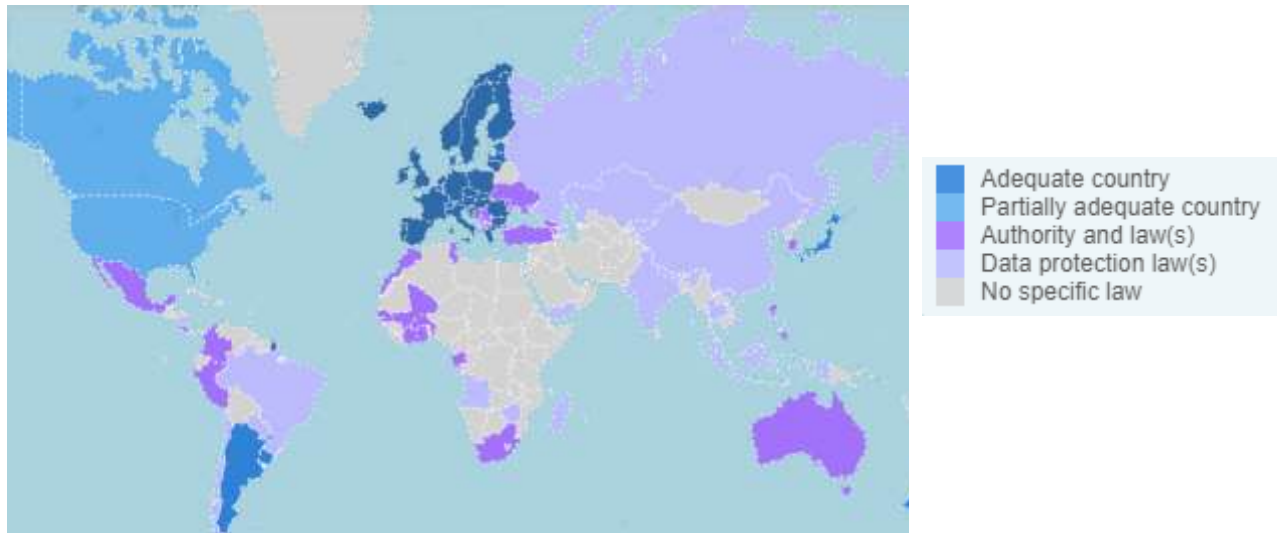
In any case, please contact the DPO first.

In which country can I transfer personal data and under which conditions?

To get an overview, consult this map:

<https://www.cnil.fr/en/data-protection-around-the-world>.

This map allows you to see the level of data protection in each country.



We train our employees and improve our internal processes.

- Data Transfer Agreement section including in our Data Processing Agreement template.
- [FAQs](#) in order to address some issues raised by the entry into force of the EU Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries.





3 Our standards in RELATIONSHIPS WITH our NETWORK and SUPERVISORY AUTHORITIES

Data Protection Officer

The Group appointed a Data Protection Officer.

Data Protection Officer or DPO assists us to monitor internal compliance, informs and advises on our data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority.

The DPO must be independent, an expert in data protection, adequately resourced, and reports to the highest management level.

DPO can help us demonstrate compliance and is part of the enhanced focus on accountability.




Tasks of the DPO	Reference OneDoc	Reference GDPR
<ul style="list-style-type: none">Our DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.	MADPGR001EN Personal Data Protection Manual	GDPR Article 39 Tasks of the data protection officer
<ul style="list-style-type: none">We will take account of our DPO's advice and the information they provide on our data protection obligations.		
<ul style="list-style-type: none">When carrying out a DPIA, we seek the advice of our DPO who also monitors the process.		
<ul style="list-style-type: none">Our DPO acts as a contact point for the Supervisory Authorities.		
<ul style="list-style-type: none">When performing their tasks, our DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.		

The Group DPO was designated to the CNIL by the CEO for taking function on 25 May 2018, the date of application of the GDPR.

Accessibility of the DPO:

- Our Data Protection Officer, Jennifer Godin, is easily accessible as a point of contact for our employees, individuals and the Supervisory Authority.
- We have published the contact details of the DPO and communicated them to the Supervisory Authorities.

✓ <https://www.Roquette.com/data-protection>



Your point of contact

Our Group Data Protection Officer is a single point of contact for our employees, individuals and the Supervisory Authorities concerning all privacy and data protection topics.

Jennifer Godin, Group Data Protection Officer
Roquette Frères, Legal & Compliance
Rue de la Haute Loge, 62136 Lestrem France

Email to DPD@roquette.com

Contact the DPO in case of:

- ✓ Personal Data Processing
- ✓ Data Subjects Requests
- ✓ Personal Data Breach
- ✓ Need for Advice or Assistance



We train our employees and improve our internal processes.



Data Protection Network

Relays into departments and Local DPOs or Coordinators are a network that enables the Group Data Protection Officer, respectively, to implement the Personal Data Protection rules in each business unit and support department, and to comply with the requirements of relevant laws and regulations data protection in the countries where the Group operates.



The Local DPOs/Coordinators shall have at least the following tasks:

- To inform and advise locally about the obligations pursuant to Roquette's Personal Data Protection Policy defined by the Roquette's Group DPO and the requirements of their local applicable laws concerning data protection;
- To monitor compliance with local legislation, with others legislations and applicable regulations concerning data protection, where required, with the assistance of the Roquette's Group DPO, and with the policies related to the protection of personal data;
- To provide advice locally where requested with regards the data protection impact assessment and monitor its performance;
- To cooperate with the local supervisory authority;
- To act as the contact point for the Roquette's Group DPO on issues relating to processing, and to consult the Roquette's Group DPO, where appropriate, with regard to any other matter;
- To report his or her activities to the Roquette's Group DPO to contribute to the Group Data Protection Management System.

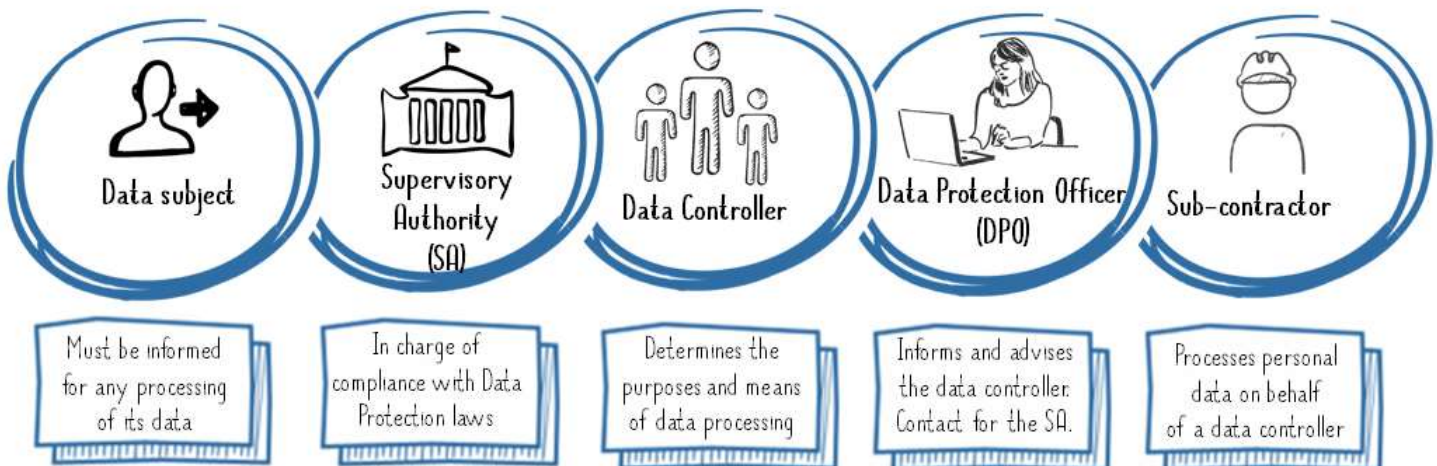
We train our employees and improve our internal processes.

Our annual PDP Seminar is the meeting place for our network of data protection and privacy contributors.

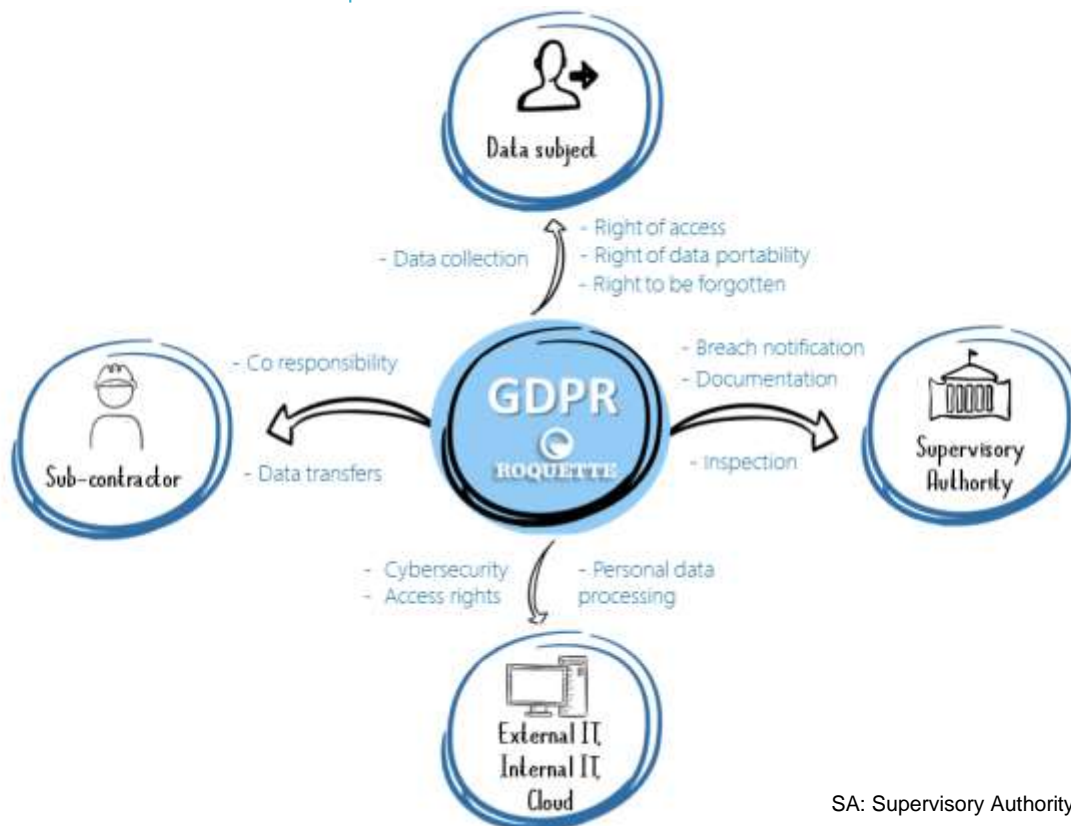


& Stakeholders

Who are the new players?



What are the relationships between these stakeholders?



SA: Supervisory Authority – See page [50](#)



Supervisory authorities

Around the world many countries have a data protection law and an independent Data Protection Authority (DPA).

These authorities are the independent national regulator for privacy and freedom of information. They promote and uphold the rights of data subjects to access organizations-held information and have their personal information protected.



What is the role of a supervisory authority in the context of the GDPR?

Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of personal data and privacy laws, in order to protect the fundamental rights and freedoms of data subjects in the scope of personal data processing and to facilitate the free flow of such personal data within the EU.

In the context of the GDPR all EU Member States have a data protection authority, in general serving as the main point of contact of stakeholders within that Member State.

In order to make sure that the GDPR is applied in a consistent way across the EU each supervisory authority has to work together with the others and with the European Commission.

Each supervisory authority on its territory must promote public awareness and understanding of the risks, rules, safeguards and rights in relation to personal data processing.

They are also the place to go to in case of a violation of data protection legislation and for advice and specific questions and/or assistance from the perspective of organizations.

In brief, the responsibilities of Supervisory Authorities (SA) are to:

- Ensure the application of the rules including through fines,
- Clarify the application of the rules, if need be, e.g. through guidelines,
- Promote a culture of dialogue with all stakeholders, including businesses,
- Cooperate together.

[CNIL](#) : Commission Nationale de l'Informatique et des Libertés - French DPA.

Lead Authority

- The supervisory authority for the main establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned.
- Identifying a lead supervisory authority is only relevant where a controller or processor is carrying out the cross-border processing of personal data.

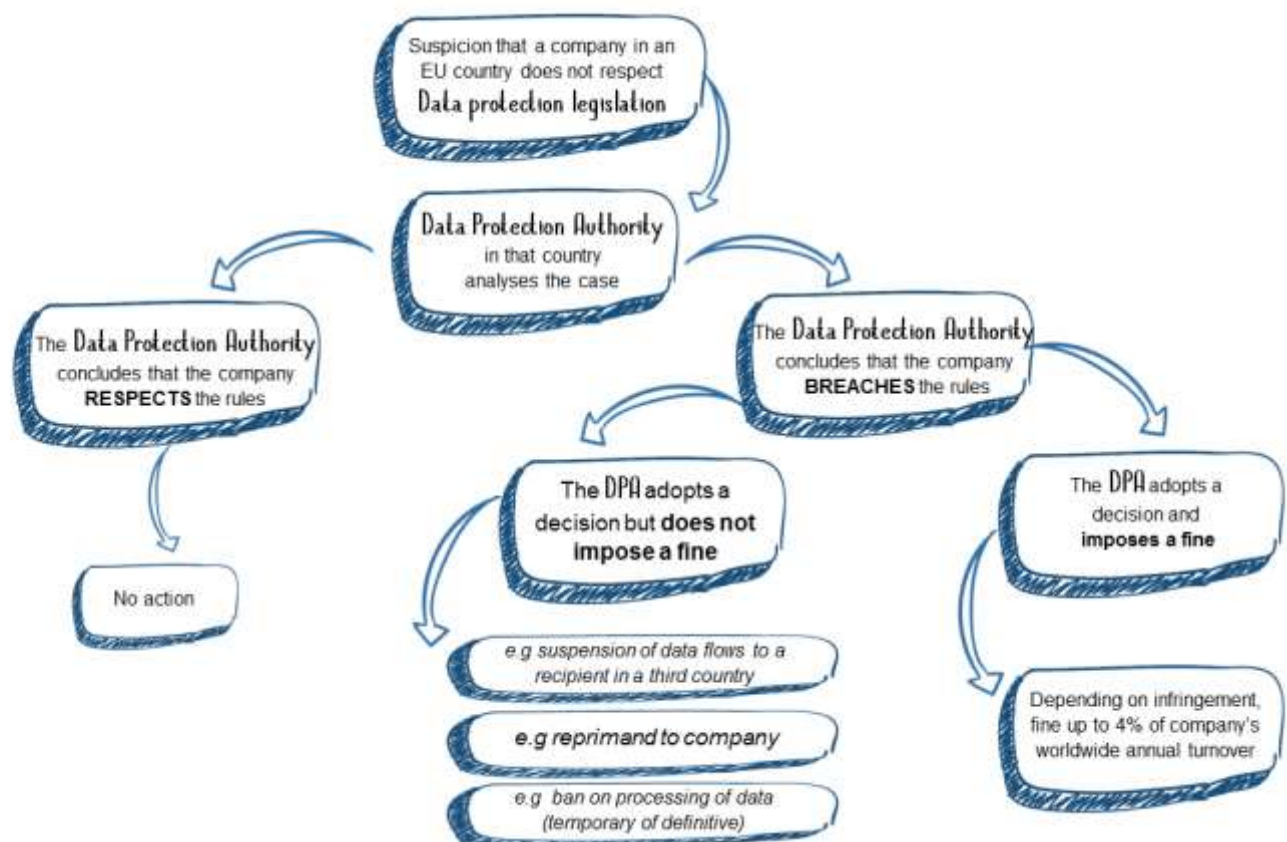
How to identify the 'lead supervisory authority'?

Identify the main controller's place of central administration in the EU.

The supervisory authority of the country where the place of central administration is located is the controller's lead authority.

The CNIL is Roquette's Lead Supervisory Authority

How does the GDPR sanction mechanism work in practice?



Governance

“The **data protection organization** is mainly structured around the **Data Protection Officer**, its coordinators per site and per function, the Chief Executive Officer as **Data Controller**, the Heads of Global Functions as responsible of the implementation of processing of personal data and the subcontractors as **Processor**.”

[MDPG001EN]

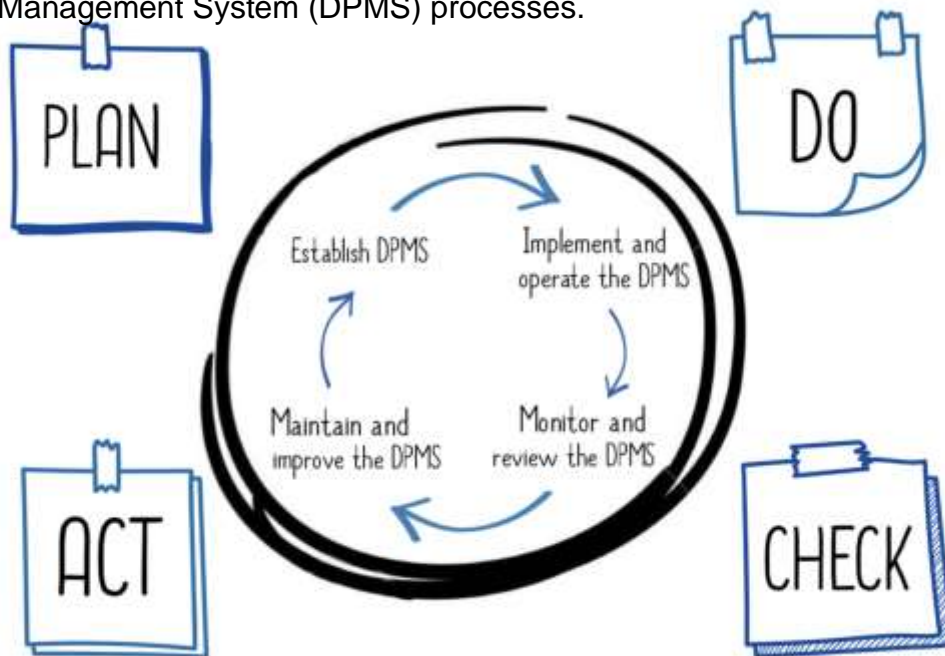


We adopt a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving Roquette's Personal **Data Protection Management System (DPMS)**.

The process and approach for personal data protection management defined in this governance encourages its users to emphasize the importance of:

- 1) understanding Roquette's data protection requirements and the need to establish directives and procedures for data protection;
- 2) implementing and operating controls to manage Roquette's data protection risks in the context of Roquette's overall business risks;
- 3) monitoring and reviewing the performance and effectiveness of the DPMS; and
- 4) continual improvement based on objective measurement.

We adopt the "**Plan-Do-Check-Act**" (**PDCA**) model, which is applied to structure all Data Protection Management System (DPMS) processes.



Our approach:

Our GDPR Compliance Program is focus on:

- Understanding how our organization collects, stores, utilizes and transfers data to ensure to be compliant,
- Creating a culture of compliance within our organization,
- Conducting privacy impact assessments,
- Preparing for a data breach,
- Allocating resources to Privacy Program,
- Implementing a Data Protection Management System (Plan – Do – Check – Act).

To achieve these objectives, we have as part of our Program:

- Defined a Data Protection Policy and associated Governance and Documentation,
- Managed a GDPR compliance project for the review of processing, the management of data breaches, the review of contracts, clauses on data protection, data transfer agreement, etc.,
- Implemented a privacy management software compliant with the GDPR.



The main features of this management platform are:

- Maintenance of the data processing register (Data Mapping),
- Risk management associated with processing (from the PIA, etc.),
- Management of requests and rights (access, rectification, opposition, etc.),
- Management of incidents and data breaches,
- Management of compliance documentation.



Accountability

Accountability is one of the data protection principles. It makes us responsible for complying with the GDPR and says that we must be able to demonstrate our compliance.

Why is accountability important?

Taking responsibility for what we do with personal data, and demonstrating the steps we have taken to protect people's rights not only results in better legal compliance, it also offers us a competitive edge. Accountability is a real opportunity for us to show, and prove, how we respect people's privacy. This can help us to develop and sustain people's trust.



Furthermore, if something does go wrong, then being able to show that we actively considered the risks and put in place measures and safeguards can help us provide mitigation against any potential enforcement action. On the other hand, if we cannot show good data protection practices, it may leave us open to fines and reputational damage.

What does it mean concretely to adhere to the principle of accountability?

The Personal Data Processing entails a duty of care and the adoption of concrete and practical measures for its protection. Adhering to the accountability principle means:

- documenting and communicating as appropriate all privacy-related directives, procedures and practices (our “Policy”);
- assigning to a specified individual within the organization (who might in turn delegate to others in the organization as appropriate) the task of implementing the Policy;
- when transferring Personal Data to third parties, ensuring that the third party recipient will be bound to provide an equivalent level of Privacy & Data Protection through contractual or other means such as mandatory internal policies (applicable law can contain additional requirements regarding international data transfers);
- providing suitable training for the personnel of the Data Controller who will have access to Personal Data;

- setting up efficient internal complaint handling and redress procedures for use by Data subject;
- informing Data Subjects about privacy breaches that can lead to substantial damage to them (unless prohibited, e.g., while working with law enforcement) as well as the measures taken for resolution;
- notifying all relevant privacy stakeholders about privacy breaches as required in some jurisdictions (e.g., the data protection authorities) and depending on the level of risk;
- allowing an aggrieved Data Subject access to appropriate and effective sanctions and/or remedies, such as rectification, expungement or restitution if a privacy breach has occurred; and
- considering procedures for compensation for situations in which it will be difficult or impossible to bring the natural person's privacy status back to a position as if nothing had occurred.

Checklist:

- ☒ We take responsibility for complying with the GDPR, at the highest management level and throughout our organization.
- ☒ We keep evidence of the steps we take to comply with the GDPR.

We put in place appropriate technical and organizational measures, such as:

- ☒ adopting and implementing data protection rules;
 - ☒ taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
 - ☒ putting written contracts in place with organizations that process personal data on our behalf;
 - ☒ maintaining documentation of our processing activities;
 - ☒ implementing appropriate security measures;
 - ☒ recording and, where necessary, reporting personal data breaches;
 - ☒ carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
 - ☒ appointing a data protection officer; and
 - ☒ adhering to relevant codes of conduct and signing up to certification schemes (where possible).
- ☒ We review and update our accountability measures at appropriate intervals.



Documentation

What is documentation?

We are required to maintain a record of our processing activities, covering areas such as processing purposes, data sharing and retention; we call this **documentation**.



Documenting our processing activities is important, not only because it is itself a legal requirement, but also because it can support good data governance and help us demonstrate our compliance with other aspects of the GDPR and data protection laws in force.

Checklist:

Documentation of processing activities – requirements

- ☑ As controller for the personal data we process, we document all the applicable information under Article 30(1) of the GDPR.
- ☑ We document our processing activities in writing.
- ☑ We document our processing activities in a granular way with meaningful links between the different pieces of information.
- ☑ We conduct regular reviews of the personal data we process and update our documentation accordingly.

Documentation of processing activities – best practice

- ☑ We document our processing activities in electronic form so we can add, remove and amend information easily.

When preparing to document our processing activities we:

- ☑ do information audits to find out what personal data our organization holds;
- ☑ use questionnaires via our Digital, Security & Privacy tools and talk to staff across the organization to get a more complete picture of our processing activities; and
- ☑ review our policies, directives, procedures, contracts and agreements to address areas such as data retention, security and sharing.

As part of our record of processing activities we document, or link to documentation, on:

- ☑ information required for privacy notices;
- ☑ records of consent when required;
- ☑ controller-processor contracts;
- ☑ the location of personal data;
- ☑ Data Protection Impact Assessment reports; and also
- ☑ records of personal data breaches;
- ☑ records of data subjects requests.

Where is our documentation on Data Protection?

ONE

Global Function
Data Protection



Privacy & Data Protection

"Data Protection is relevant to and the responsibility of everyone in our organization"

Content

- Laws and regulations
- Information and awareness
- Best practises and policies

CULTURE

ONE

Community
Data Protection Network



Data Protection
Network

"We are all actors in the protection of personal data"

Content

- Personal Data Protection Policy
- Data Protection Management System
- Local Legislation
- Human resources
- Global Digital
- Legal & Compliance
- Internal Audit & Control
- GBU & Commercial
- Innovation, R&D
- Global Security
- Insurance & Risk Management

COMPLIANCE

OneTrust

Privacy Management Software



"Our Privacy Management tool dedicated to Privacy Security & Third Party Risk"

Modules



Data Mapping
Automation



PIA & DPIA
Automation



Subject
Access
Request
Portal



Incident &
Breach
Management

ACCOUNTABILITY



Privacy Impact Assessment

Privacy Impact Assessment or **PIA** is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.

The acronym "**PIA**" is used interchangeably to refer to **Privacy Impact Assessment** and **Data Protection Impact Assessment (DPIA)**.

How is a PIA carried out?

The compliance approach implemented by carrying out a PIA is based on two pillars:

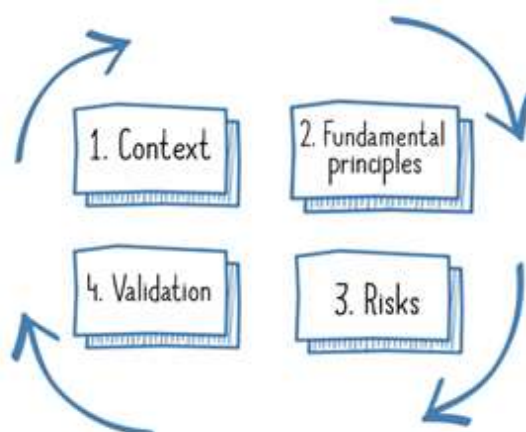
- 1) **fundamental rights and principles**, which are “non-negotiable”, established by law and which must be respected, regardless of the nature, severity and likelihood of risks;
- 2) **management of data subjects’ privacy risks**, which determines the appropriate technical and organizational controls to protect personal data.



Compliance approach using a PIA

To summarise, to carry out a PIA it is necessary to:

- 1) define and describe the **context** of the processing of personal data under consideration;
- 2) analyse the controls guaranteeing compliance with the **fundamental principles**: the proportionality and necessity of processing, and the protection of data subjects' rights;
- 3) assess privacy **risks** associated with data security and ensure they are properly treated;
- 4) formally document the **validation** of the PIA in view of the previous facts to hand or decide to revise the previous steps.



General approach for carrying out a PIA

This is a continuous improvement process. Therefore, it sometimes requires several iterations to achieve an acceptable privacy protection system. It also requires a monitoring of changes over time (in context, controls, risks, etc.), for example, every year, and updates whenever a significant change occurs.

The approach should be implemented as soon as a new processing of personal data is designed. Implementing this approach at the outset makes it possible to determine the necessary and sufficient controls and thus to optimize costs. Conversely, implementing it after the creation of the system and the implementation of controls may call into question the choices made.

Our responsibilities:

- Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, Roquette as controller, shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
- The project owner shall seek the advice of the Data Protection Officer designated when carrying out a data protection impact assessment.

Rules	Reference OneDoc	Reference GDPR
<ul style="list-style-type: none"> • Carry out a PIA in case of high risk 	DIDPGRO03EN Rule 1	Art. 35
<ul style="list-style-type: none"> • Content of a PIA 	DIDPGRO03EN Rule 2	
<ul style="list-style-type: none"> • Tasks of the DPO concerning PIA 	DIDPGRO03EN Rule 3	
<ul style="list-style-type: none"> • Review of PIA 	DIDPGRO03EN Rule 4	

We train our employees and improve our internal processes. and improve our internal processes.

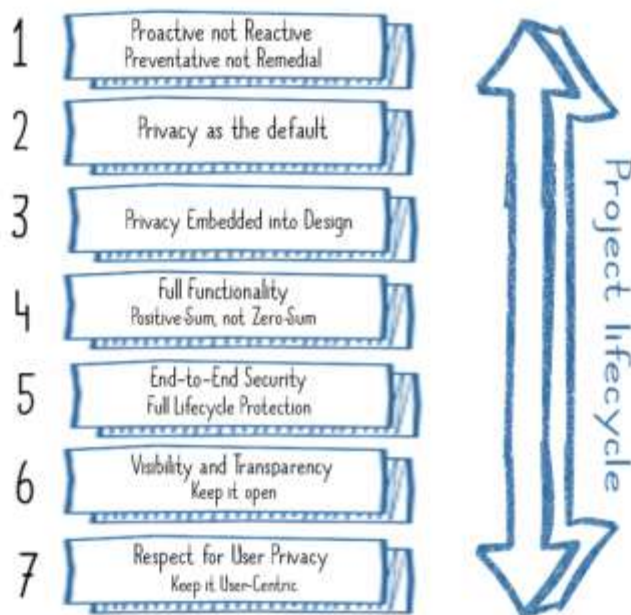
- Learning on Security & Privacy Review into Projects & Contracts.
- Privacy Impact Assessment template launch automatically in our Privacy Management Software OneTrust@Roquette when required.

To know more: CNIL [PIA Methodology](https://www.cnil.fr/en/home), 2018 edition - <https://www.cnil.fr/en/home>



Privacy by Design & by Default

Privacy by Design means building privacy into the design, operation, and management of a given system, business process, or design specification.



What is Data Protection by Design?

Data protection legislation contains basic principles for safeguarding the privacy of data subjects.

Data protection by design and by default helps ensure that the information systems we use fulfil these data protection principles, and that the systems safeguard the rights of data subjects.

We consider that:

Roquette relies on information systems and databases to perform a range of operational and administrative tasks. A great part of those information systems process personal data, therefore their full compliance with the regulation is of utmost importance.

Businesses that take data protection issues seriously, build trust.

Thus, strong data protection measures can be a competitive advantage.

Management commitment is crucial for making the decision to apply the principles of data protection by design in the organization's procurements and software development.

Management must also ensure to provide sufficient resources for this task.

Taking data protection into account throughout the development process is both cost-effective and more efficient than making changes to an existing piece of software.

Our responsibilities:

Under the GDPR, data protection by design is, for the first time, became a legal obligation. This will mean that data protection and privacy must be built in to the design specifications and architecture of information and communication systems and technologies.

Roquette as data controller must comply with the requirements governing data protection by design during software development, and when ordering systems, solutions, and services.

The requirements must accordingly also be included when entering into agreements with suppliers, and when using consultants (cf. our standards with subcontractors).

Rule	Reference OneDoc	Reference GDPR
<ul style="list-style-type: none">• Security, Privacy & Data Protection by design and by default	DIDPGR007EN Rule 3	Art. 25

Checklist:

- ✓ Review the Data Protection Impact Assessment (DPIA)
- ✓ Avoid, limit, or minimize the need to collect and process sensitive personal data
- ✓ Limit and minimize the exposure of unnecessary functionality and personal data in the user interface
- ✓ Anonymize or pseudonymize personal data wherever possible
- ✓ All privacy-friendly configurations need to be on by default
- ✓ Tracking from one website to another should be disabled by default
- ✓ Withdraw consent via a menu within the software. Keep in mind that collection of personal data must cease if consent is withdrawn
- ✓ Settings should be presented in a menu where the data subject must make a conscious choice to actively “change” to less privacy-friendly settings
- ✓ Device tracking should be disabled by default

We train our employees and improve our internal processes.

- Guideline on our Community “Data Protection Network”.
- Methodologies: Security & Compliance review into projects & contracts.
- Learning on HR platform.



Data Breach notification

What is a personal data breach?

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

This means that a breach is more than just losing personal data.



Examples:

- Loss of a client database
- Disclosure of employees performance appraisal

Our responsibilities:

We have to apply rules to treat any breach of personal data in such a way as to limit its impact on the data subjects and to prevent this from happening again.

Rules	Reference OneDoc	Reference GDPR
• Notification of a personal data breach to the Data Protection Officer.	DIDPGRO08EN Rule 1	Art. 33
• Notification of a personal data breach to the supervisory authority.	DIDPGRO08EN Rule 2	
• Communication of a personal data breach to the data subject.	DIDPGRO08EN Rule 3	Art. 34

How much time do we have to report a breach?

We must report a notifiable breach to the Supervisory Authority without undue delay, but not later than 72 hours after becoming aware of it.

What breaches do we need to notify the relevant supervisory authority about?

We only have to notify the relevant supervisory authority of a breach if it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals. For example:

- result in discrimination;
- damage to reputation;
- financial loss; or
- loss of confidentiality or any other significant economic or social disadvantage.

We have to assess this on a case by case basis and we need to be able to justify your decision to report a breach to the supervisory authority.

When do we have to notify individuals?

If a breach is likely to result in a **high risk** to the rights and freedoms of individuals, we must notify those concerned directly without undue delay.

The duty to notify an individual about a breach does not apply if:

- we have implemented appropriate technical and organizational measures which were applied to the personal data affected by the breach;
- we have taken subsequent measures which will ensure that any high risk to the rights and freedoms to individuals is no longer likely to materialize; or
- it would involve disproportionate effort.

Where a communication of a breach would involve disproportionate effort, we must make the information available to individuals in another, equally effective way, such as a public communication.

Whom should we contact in case of Data Breach?

Please contact the **Data Protection Officer** at dpo@Roquette.com and/or report incident by our "[Privacy Alert](#)" web form.

If you need to report a potential compliance violation you can get in touch with your usual point of contact or report a problem through the confidential Roquette alert device: [Speakup](#)®.

SpeakUp®



Privacy alert

How to report a privacy incident?

[Report incident](#)



Monitoring & Review

We consider that:

Roquette is committed to:

- ☑ ensure a legal and technological **monitoring** on data protection requirement,
- ☑ **review** and **improve** our Data Protection Management System (DPMS)

in order to take into account regulatory and technological evolutions as well as the internal constraints of services. [DIDPGRO09EN]



Our responsibilities:

Rules

	Reference OneDoc	Reference GDPR
<ul style="list-style-type: none"> Ensure a legal and technological monitoring and review on the protection of personal data 	DIDPGRO09EN Rule 1	Best Practices
<ul style="list-style-type: none"> Regularly monitor the implementation of the DPMS and data protection directives 	DIDPGRO09EN Rule 2	
<ul style="list-style-type: none"> Regularly review the personal data protection policy and the documentation of the DPMS 	DIDPGRO09EN Rule 3	

We train our employees and improve our internal processes.

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

pdp Privacy & Data Protection
News



Audit Management

Manage Internal/External Audits

Design and support our Privacy Program

Regulatory Research Software:

We use a platform providing a suite of privacy solutions designed to help us monitor regulatory developments, mitigate risk and achieve global compliance:

- ☑ Regulatory tracking
- ☑ Comparative cross-border charts
- ☑ Guidance notes
- ☑ GDPR portal
- ☑ Templates and checklists
- ☑ Ask an analyst service
- ☑ Legal research

Audit & Review of the Data Protection Management System:

We conduct internal audits to determine whether inputs of the DPMS are:

- ☑ compliant to the requirements of this Guide, the Policy and applicable legislation or regulations;
- ☑ are effectively implemented and maintained; and
- ☑ performed as expected.

We undertake a management review of the DPMS to ensure that the scope remains adequate and improvements in the DPMS process are identified.

In order to do that, inputs are:

- ☑ Objectives, controls, processes and procedures of the DPMS;
- ☑ Results of previous compliance audits and controls;
- ☑ Feedback from interested parties;
- ☑ Techniques, products or procedures, which could be used in the organization to improve the DPMS performance and effectiveness;
- ☑ Status of preventive and corrective actions;
- ☑ Vulnerabilities or threats not adequately addressed in the previous risk assessment;
- ☑ Results from effectiveness measurements;
- ☑ Follow-up actions from previous management reviews;
- ☑ Any changes that could affect the DPMS; and
- ☑ Recommendations for improvement.



Reference documents

- [[Code of Conduct](#)] Roquette Group Code of Conduct
- [GDPG001EN] Glossary of definitions relating to Data Protection
- [MDPG001EN] Personal Data Protection manual
- [DIDPGR001EN] Directive on culture of respect of privacy and data protection
- [DIDPGR002EN] Directive on lawfulness of personal data processing
- [DIDPGR003EN] Directive on privacy impact assessment
- [DIDPGR004EN] Directive on processing of sensitive data
- [DIDPGR005EN] Directive on records of processing activities
- [DIDPGR006EN] Directive on compliance with the rights of persons
- [DIDPGR007EN] Directive on security of personal data
- [DIDPGR008EN] Directive on notification of a personal data breach
- [DIDPGR009EN] Directive on review of personal data protection management system
- [DIDPGR010EN] Directive on Privacy & Data Protection in Alert Management System
- [DISUGR001EN] Directive on Information Protection & Confidentiality

Bibliography

[[EU Charter](#)] Charter of Fundamental Rights of the European Union, 2010/C 83/02.

[[GDPR](#)] 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

[[DP-Act](#)] French Data Protection Act no. 78-17 of 6 January 1978, amended.

[[WP29 – Guidelines](#)] Guidelines for identifying a controller or processor's lead supervisory authority | WP 244 rev.01 (5 April 2017).

[[WP29- Guidelines](#)] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 | WP 248 rev.01 (13 October 2017).

[[WP29- Guidelines](#)] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 | WP 253 (21 October 2017).

[[WP29- Guidelines](#)] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 | WP 251 rev.01 (13 February 2018).

[[WP29 – Guidelines](#)] Guidelines on Data Protection Officers ('DPOs') | WP 243 rev.01 (5 April 2017).

[[WP29- Guidelines](#)] Guidelines on Transparency under Regulation 2016/679 | WP260 rev.01 (11 April 2018).

[[WP29- Guidelines](#)] Guidelines on Consent under Regulation 2016/679 | WP259 rev.01 (11 April 2018).

[[EDPB – Opinion](#)] Opinion 23/2018 on Commission Proposals on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (Art. 70.1.b) (26 September 2018).

[[EDPB – Opinion](#)] Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data in Japan (5 December 2018).

[[EDPB – Opinion](#)] Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR) (12 July 2019).

[[EDPB- Recommendation](#)] Recommendation 01/2019 on the Draft List of the European Data Protection Supervisor Regarding the Processing Operations Subject to the Requirement of a Data Protection Impact Assessment (Article 39(4) of Regulation (EU) 2018/1725) (10 July 2019).

[[EDPB – EDPS Joint Response](#)] EPDB-EDPS Joint Response to the LIBE Committee on the Impact of the US Cloud Act on the European Legal Framework for Personal Data Protection (Annex) (10 July 2019).

[[EDPB Opinion](#)] Opinion 13/2019 on the draft list of the competent supervisory authority of France regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR) (10 July 2019).



Sources

- Commission Nationale de l'Informatique et des Libertés
 - <https://www.cnil.fr/en/home>
 - May 2022
 - License: [CC-BY-ND 3.0 FR](#)
- Information Commissioner's Office
 - <https://ico.org.uk/>
 - May 2022
 - Licensed under the [Open Government Licence](#)
- European Union
 - <https://eur-lex.europa.eu>
 - 1998-2022
- <https://www.iso.org/home.html>
- <https://www.dataguidance.com/>
- <https://www.onetrust.com/>
- <https://www.corporatefiction.fr/>
- <https://pixabay.com/fr/service/license/>

These sources are only and strictly used for educational purposes, learning and awareness-raising.

The actors mentioned do not endorse nor make any warranties about the contents of this work.

The intellectual property rights, including copyright in its materials still belong to them.

The English version of this Guide is the reference.
Translations of this document may be subject to interpretation.
First edition: September 2019
Second edition: May 2022
Published by ROQUETTE FRERES
Author: Jennifer Godin, Data Protection Officer
Editorial design and graphics: Compliance Office
Photography: free to use

All rights reserved. No part of this document may be reproduced or utilized in any form by any means, electronic or mechanical, including photocopying, scanning, recording, or by information storage or retrieval systems, without express permission in writing to dpo@roquette.com.

Authorized external use.



