Privacy policy

Last update : **June 30, 2026**

The Dalkia company is very committed to respecting the privacy of individuals and to the protection of the personal data it processes in the context of its activities and the services it provides. As such, the Dalkia company ensures that it acts in accordance with all regulations in force applicable to the protection of personal data and in particular with EU Regulation No. 2016/679 of April 27, 2016 relating to the protection of natural persons with regard to the processing of personal data and the free movement of these data (GDPR) and Law No. 78-17 of January 6, 1978 relating to data processing, files and freedoms (LIL).

The purpose of this personal data protection policy is to inform, in a clear, concise and understandable manner, of the conditions for implementing the processing of personal data carried out by the company Dalkia, acting as data controller and to inform all persons concerned of the Data Protection and Liberties rights they hold as well as how to exercise them. It is aimed in particular at visitors to the website www.dalkia.fr and www.dalkia.com , to customers and prospects of the Dalkia company, to suppliers as well as to people wishing to apply for a job or internship offer. Depending on the particular purpose of processing, it may also be aimed at other specific categories of data subjects.

1. Definitions

GDPR : Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and any other subsequent text of French law including its implementing texts

LIL : French “Informatique et Libertés” law of January 6, 1978 amended.

Personal data : any data relating to an identified or identifiable natural person; is deemed to be an “identifiable natural person” 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 specific elements specific to their physical, physiological, genetic, psychological, economic, cultural or social identity

Processing : within the meaning of the GDPR, “processing” corresponds to any operation or set of operations carried out or not using automated processes and applied to personal data, such as collection, recording, organization , structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, reconciliation or interconnection, limitation , erasure or destruction

Data Controller : the natural or legal person, public authority, service or other body which, alone or jointly with others, determines the purposes and means of the processing

Data Processor : the natural or legal person, public authority, service or other body which processes personal data on behalf of the controller

Data subject : these are the natural persons whose personal data are subject to processing.

DPO : the Data Protection Officer, or Data Protection Delegate in French, is the person responsible for ensuring the protection of personal data within the organization which designated him and for monitoring compliance with the regulations in force and applicable to the protection of personal data

2. Who is responsible for the processing carried out on your personal data?

The person responsible for processing personal data covered by this Privacy policy is:

DALKIA SA – Tour Europe – 33, place des corolles – TSA 77655 - 92099 Paris La Défense Cedex

3. What are the different processing activities of your personal data that can be implemented by Dalkia? (The objectives pursued? The legal justifications? The data retention periods?)?

In accordance with applicable regulations, Dalkia ensures compliance with all general principles applicable to the processing of personal data.

As such, Dalkia ensures in particular that:

- Personal data is only collected for explicit purposes, determined in advance and undertakes not to subsequently process them in a manner incompatible with these purposes;
- Only personal data strictly necessary for the pursuit of the purpose of the processing can be collected and ensures for each processing that it can validly invoke one of the legal bases authorizing the implementation of processing of personal data. When the provision of personal data is mandatory and conditions the conclusion of a contract, Dalkia ensures that the persons concerned are informed in advance;
- Personal data does not be kept only for a period not exceeding that necessary for the purposes for which they are processed.

To be as transparent as possible with regard to the processing of personal data concerning you, you will find below a table containing all the processing carried out by the company Dalkia acting as data controller, with the different purposes of the processing. , the legal bases allowing their implementation as well as the retention periods of the data applied.

Processing activities	Purposes of processing	Legal bases	Retention period
Website management www.dalkia.fr and www.dalkia.com	Process requests for information or connection with a specific service received via contact forms	Art. 6.1a of the RGPD: the consent of the person concerned	3 months
	Process requests to download Dalkia white papers		
	Analyze visitor behavior, measure the audience and establish website traffic statisticswww.dalkia.fr	Art. 6.1f of the GDPR: The processing is necessary for the purposes of the legitimate interests pursued by Dalkia which are to assess the performance of its website, to understand the behavior of Internet users, to determine the effectiveness of the strategies implemented within the framework of 'a process of continuous improvement of the user experience	25 months
Management of commercial activities	Manage contracts (management of orders, delivery, execution of the service or supply of goods, invoices and payments)	Article 6.1 b of the GDPR: Processing is necessary for the performance of a contract or the execution of pre-contractual measures	Personal data is kept for 10 years from the end of the contractual relationship
	Monitor customer relations	Article 6.1 b of the GDPR: Processing is necessary for the performance of a contract	
	Carry out commercial statistics and satisfaction surveys	Art. 6.1f of the GDPR: The processing is necessary for the purposes of the legitimate interests pursued by Dalkia which are to develop its commercial strategy and guide its commercial actions taking into account the results of the studies	
	Carry out commercial prospecting actions	Art. 6.1f of the GDPR: Processing is necessary for the purposes of the legitimate interests pursued by Dalkia which are to develop its customer base by presenting and offering its services to professional prospects or to offer its customers new products or services similar to those already provided	3 years from their collection for non-customer prospects
	Manage complaints and monitor quality actions	Article 6.1 b of the GDPR: Processing is necessary for the performance of a contract	Personal data is kept for 5 years from the end of the contractual relationship
Procurement management (excluding energy purchases)	Operational procurement management: Manage the entire procurement lifecycle, from request to receipt and payment, ensuring smooth operations and compliance with contracts	- Article 6.1 b of the GDPR: Performance of a contract for the data of suppliers and their representatives necessary for the performance of contracts for the supply of goods or services - Article 6.1 f of the GDPR: Legitimate interest in processing data necessary for the administrative and logistical management of orders, including delivery tracking and dispute resolution, where such processing is not strictly related to the performance of the contract but contributes to the smooth running of the business	- Accounting and tax documents (invoices, purchase/delivery orders): 10 years from the end of the relevant accounting period, pursuant to the French Commercial Code (articles L123-22 and L123-22-1) and the French General Tax Code (article L102 B) - Data relating to the performance of the contract (excluding accounting documents): Up to 5 years after the end of the contractual relationship. This period corresponds to the general statute of limitations for commercial matters (article 2224 of the French Civil
	Supplier relationship management: Establish, maintain and develop effective and sustainable relationships with suppliers, evaluate their performance and manage risks	- Article 6.1 b of the GDPR: Performance of a contract for data necessary for monitoring contractual obligations - Article 6.1 f of the GDPR: Legitimate interest for supplier evaluation, handling	

		of non-contractual disputes, audit management, and continuous improvement of purchasing processes	Code), during which legal action may be taken. - Data and documents necessary for Dalkia to defend itself in the event of a claim under the ten-year warranty, or to activate it against its own subcontractors or suppliers, are kept for 10 years from the date of acceptance of the work. - For unsuccessful bidders: 3 years after the end of the tendering process.
	Sourcing and tendering: Identifying and selecting the best potential suppliers to meet the company's needs, organizing consultations and tenders	- Article 6.1 b of the GDPR: Performance of pre-contractual measures when processing is necessary for entering into a future contract - Article 6.1 f of the GDPR: Legitimate interest in prospecting for new suppliers, creating databases of potential suppliers, and managing applications for tenders	
	Strategic procurement management (spending analysis, cost optimization, risk management)	Art. 6.1f du RGPD : Intérêt légitime pour l'agrégation et l'analyse de données (souvent pseudonymisées ou anonymisées) afin de réaliser des reportings, des tableaux de bord, des analyses de tendances, des prévisions et des stratégies d'achat. Il s'agit d'améliorer l'efficacité et la performance globale de la fonction achats	
Dalkia facilities management	Energy management of facilities (Modeling and optimization)	Article 6.1 b of the GDPR: Processing is necessary for the performance of a contract	The data is retained for the duration of the contract. It is then archived for 10 years after the contract's termination date in the event of a claim regarding the proper execution of the R&M contract. During data archiving, the data will be anonymized.
	Management of maintenance of technical installations and work on customer sites		
	Conducting safety audits of industrial and commercial facilities	Article 6.1f of the GDPR: The processing is necessary for the purposes of the legitimate interests pursued by Dalkia, which are to protect its assets against malicious acts and to ensure the security of its property.	5 years after the date of completion of the audit or the contract concluded with the client
Communication management	Carry out internal or external communication actions (newsletters, interviews, professional directory, “Energies le mag” magazine, mailing list, etc.)	Art. 6.1a and 6.1f of the GDPR: depending on the situation, data subjects are informed at the time of collection of their personal data whether their consent is required or whether the processing is necessary for the purposes of the legitimate interests pursued by Dalkia	Personal data is kept until the person concerned objects.
	Organize and manage events		Personal data is kept until actions related to the event are closed.

Partnership management	Centralize, verify and monitor partnerships (sponsorships and sponsorships)	Article 6.1 b of the GDPR: Processing is necessary for the performance of a contract	Personal data is kept for 5 years from the end of the contractual relationship
Managing GDPR compliance obligations	Process, respond and monitor requests to exercise IT and Freedoms rights	Art. 6.1c of the GDPR: The processing is necessary to comply with a legal obligation to which Dalkia is subject: Art. 15 to 22 of the GDPR	Personal data is kept for 5 years from the closing of the file The identity documents possibly transmitted are: -Immediately deleted when the request did not require the transmission of an identity document - Deleted following completion of the identity check
	Notify the persons concerned of the occurrence of a personal data breach likely to create a high risk for their rights and freedoms	Art. 6.1c of the GDPR: The processing is necessary to comply with a legal obligation to which Dalkia is subject: Art. 33 and 34 of the GDPR	Data relating to a personal data breach notification is kept for ten years from the closure of the file
Third-party evaluation in the context of a business relationship	Verification of the third party's honorability and integrity through an assessment of their intrinsic qualities (criminal records, sanctions, reputation, etc.) and verification of the integrity of the business relationship (before and during the entire contractual relationship)	Art. 6.1c of the GDPR: The processing is necessary to comply with a legal obligation to which Dalkia is subject : The law No. 2016-1691 of December 9, 2016 relating to transparency, the fight against corruption and the modernization of economic life (“Sapin 2 Law”)	The data is kept for 5 years after the termination of the business relationship or after the date of completion of the evaluated transaction.
Fraud management	Fraud risk prevention (Fraud risk assessment and awareness campaigns) Collection and processing of suspected fraud reports (management of inquiries, investigations, and amicable, legal, and disciplinary procedures) Management, reporting, and monitoring of the anti-fraud system	Art. 6.1f of the GDPR: Processing is necessary for the purposes of the legitimate interests pursued by Dalkia which are to prevent, limit or stop any voluntary act allowing illegitimate profit or to circumvent legal obligations or internal rules	Up to 6 months from the issuance of the alert which is not relevant 5 years from the closure of the fraud file for relevant alerts
Management and processing of local professional alerts without using the WHISPLI tool provided by EDF	Provide a system for collecting and processing professional alerts in accordance with : - The law No. 2016-1691 of December 9, 2016 relating to transparency, the fight against corruption and the modernization of economic life (“Sapin 2 Law”) aimed at revealing a breach of a specific rule - The Law n°2017-399 of March 27, 2017 relating to the duty of vigilance	Art. 6.1c of the GDPR: The processing is necessary to comply with a legal obligations to which Dalkia is subject: - Art. 8.III and 17.II.2° of the “Sapin 2” law - Art. L. 225-102-4 of the commercial code, resulting from the so-called “duty of vigilance” law	- Data relating to an alert considered by Dalkia as not falling within the scope of the system are destroyed without delay - When no action is taken on an alert falling within the scope of the system, the data relating to this alert are destroyed by Dalkia, within two months from the end of the verification operations - When disciplinary or litigation proceedings are initiated against a person accused or the author of an abusive alert, the data relating to the alert may be kept by Dalkia until the end of the procedure or the limitation period for
	Make available a system for collecting and processing “ethical alerts” not imposed by law and aimed at revealing a breach of a specific rule provided for in the Dalkia’s “Ethics and Compliance” code of conduct	Art. 6.1f of the GDPR: Processing is necessary for the purposes of the legitimate interests pursued by Dalkia, which are to preserve its culture of integrity and maintain its good reputation.	

			appeals against the decision NB: Dalkia may keep the data collected in the form of intermediate archives for the time necessary to protect the whistleblower or to identify ongoing violations.
Management of the Gifts & Invitations registry	Establish a register listing gifts, invitations, or other benefits (received, offered, or refused) to facilitate monitoring and better prevent and detect acts of corruption	Art. 6.1c of the GDPR: The processing is necessary to comply with a legal obligation to which Dalkia is subject : The law No. 2016-1691 of December 9, 2016 relating to transparency, the fight against corruption and the modernization of economic life (“Sapin 2 Law”)	5 years in active storage and up to 30 years in intermediate archiving
Management of administrative investigations required for employees of its subcontractors within the framework of sensitive and classified contracts as defined by regulations	- Creation and maintenance of documents necessary for administrative investigations and their transmission to the authorizing authorities - Granting access to protected or classified information as needed.	Article 6.1c of the GDPR: The processing is necessary to comply with the security obligations imposed on Dalkia by French regulations on the Protection of National Defense Secrets. This framework is primarily based on: • The Defense Code (Legislative and regulatory parts). • The Penal Code (Protection of the fundamental interests of the Nation). • Interministerial General Instruction No. 1300 (IGI 1300).	- Primary Security Clearance (PSC): Maximum 4 years (3 years validity + 1 year administrative retention) - "Secret" level clearance: Maximum 8 years (7 years validity + 1 year administrative retention) - "Top Secret" level clearance: Maximum 6 years (5 years validity + 1 year administrative retention) - File in case of clearance refusal: Maximum 1 year after notification of the negative decision
Staff recruitment management	Allow anyone to create a personal candidate account on the Dalkia job site	Article 6.1 b of the GDPR: Processing is necessary for the execution of pre-contractual measures	2 years from the last contact with the person concerned NB: To protect against possible discrimination litigation, certain data necessary for evidentiary purposes may be kept in intermediate archiving and up to 5 years from the date of the hiring decision.
	Process applications and manage interviews in order to assess a candidate's ability to hold a job and measure their professional skills		
	Carry out tests to assess the candidate's personality or their knowledge of workplace safety	Article 6.1 f of the GDPR: Processing is necessary for the purposes of the legitimate interests pursued by Dalkia which are: - to evaluate the match between the personality of the candidate and the expectations sought for the position to be filled and the company; - to promote the well-being and safety of employees at work	

	Use of a recruiter matching feature integrated into the recruitment software allowing the automated ranking of applications received in response to a job offer (This feature is only used if the number of applications received for a job offer exceeds a certain threshold and may lead to the adoption of a fully automated decision to reject an application as part of an initial sorting)	Article 6.1 f of the GDPR: The processing is necessary for the purposes of the legitimate interests pursued by Dalkia, which are to: - Reduce the processing time of applications by selecting relevant candidates more quickly - Analyse in depth only relevant CVs - Recruit the right people for the right position with limited risk-taking With regard to the adoption of a fully automated decision, the exception referred to in Article 22.2.a of the GDPR applies: the processing is necessary for the conclusion of an employment contract In order to establish an automated ranking of applications received in response to a job offer, from the most relevant to the least relevant, the tool used only takes into account the professional skills of the candidate and their ability to occupy the position offered and this in an unbiased manner and according to objective and relevant criteria, thus reducing recruitment bias. For example, characteristics such as gender, ethnicity and age are not used, which promotes diversity and inclusion.	
	Build a CV library with the aim of contacting relevant profiles in order to present them with job offers	Art. 6.1a of the RGPD: the consent of the person concerned	
	Carry out campaigns targeting potential candidates for the purpose of promoting Dalkia job advertisements		12 months
	Consultation of profiles on publicly accessible online sources (professional social network such as LinkedIn and other sites dedicated to employment) in order to identify potential candidates likely to be interested in a job offer	Article 6.1 f of the GDPR: The processing is necessary for the purposes of the legitimate interests pursued by Dalkia which are to promote and improve its recruitment by searching for profiles of potential candidates on professional social networking platforms and other sites dedicated to employment.	The data consulted is not retained
	Recording of information relating to a profile available on publicly accessible online sources (professional social network such as LinkedIn and other sites dedicated to employment) with a view to building up a pool of potential candidates enabling applications to be generated (indirect collection of identification data, contact data and data relating to professional life)	Art. 6.1a of the GDPR: the consent of the data subject	2 years (3 months in the absence of consent from the person contacted or in the event of impossibility of obtaining consent in the absence of a contact email address)

Managing reception and monitoring of external visitors on site	Ensuring the safety of property and people, as well as controlling access to the premises	Article 6.1 f of the GDPR: The processing is necessary for the purposes of the legitimate interests pursued by Dalkia, which are to ensure the security of property, people (employees and visitors) and confidential information present on the site	3 months
Dispute management (excluding claims and social disputes)	Instruction and response to received requests Monitor and handle disputes before the courts	Article 6.1 b of the GDPR: Processing is necessary for the performance of a contract	Personal data is in principle kept for the duration of the litigation procedure and until the limitation periods for actions that could be initiated have expired
Management and monitoring of relationships with legal professionals	Establishment of lists of preferred legal professionals Management of contractual relationships with the legal professionals involved	Article 6.1(f) of the GDPR: Processing is necessary for the purposes of the legitimate interests pursued by Dalkia, which are to structure and optimize the use of legal professionals capable of supporting the legal department. Article 6.1(b) of the GDPR: Processing is necessary for the performance of a contract or pre-contractual measures.	Personal data is kept for the entire duration of the contractual relationship and up to 5 years, in intermediate archiving, from the end of the contractual relationship

4. Who has access to your personal data?

In order to be able to provide its services and within the strict framework of each purpose of the processing implemented by the company Dalkia, the following categories of recipients are likely to receive communication of personal data:

- Internal personnel of the Dalkia company, subject to an obligation of confidentiality and specially authorized to process personal data with regard to their functions
- The various suppliers, commercial partners and technical service providers of the Dalkia company, specially authorized to process personal data on its behalf and in accordance with the requirements of the applicable regulations
- Authorities legally authorized within the framework of their missions or the exercise of a right of communication

5. How do we secure your personal data?

Dalkia has an Information Systems Security Policy (PSSI). The group's information systems security manager is responsible for its deployment within the group.

Dalkia implements a set of measures recognized as relevant by IT security experts to ensure a good level of protection of Information Systems and in particular:

- protection against viruses and malware,
- network monitoring,
- protection against intrusions,
- software updates,
- securing premises,
- protection of workstations and servers.

Dalkia regularly develops and strengthens these systems by adapting them to technological possibilities and new vulnerabilities identified. The behavior and vigilance of each user is also a key element of IT asset security. To do this, each user of the information system must respect the Dalkia IT charter. This is updated whenever safety or PDP regulations evolve significantly.

Dalkia has implemented security control measures.

All these security measures are intended to ensure that this data is adequately protected against unauthorized access, modification, disclosure or destruction of the processed data.

These measures include the following:

Dalkia employees, subcontractors, service providers and contacts who need access to your personal data to exercise their roles, functions and responsibilities:

- are authorized and have access strictly reserved for them;
- are made aware and/or trained, according to their roles, functions and responsibilities;
- have signed, according to their functions and responsibilities, a confidentiality undertaking and have been informed of the risks and sanctions in the event of failure to comply with this obligation.

We encrypt data when necessary.

We regularly carry out audits of our suppliers processing personal data on our behalf as well as internal audits.

Dalkia ensures that third parties, service providers and subcontractors within the meaning of GDPR respect and apply appropriate security measures.

6. Are personal data subject to transfer to a country outside the European Union?

As a matter of principle, Dalkia strives to minimize situations in which personal data could be transferred to a country outside the European Union. However, it may happen that the use of services provided by a service provider or a third-party application may involve, within the meaning of the regulations, a transfer of data to a country located outside the European Union. In these situations, Dalkia will ensure that processing involving a transfer of data outside the European Union can only take place provided that it ensures a sufficient and appropriate level of protection of your personal data. As such, Dalkia, with the support of its data protection delegate, will use one of the mechanisms provided for by the regulations to regulate these transfers, unless it is possible to benefit from an exemption. in particular situations and under specific conditions.

However, following recent developments in European jurisprudence and in particular the invalidation of the "Privacy Shield" (Agreement which allowed the transfer of data between the European Union and American operators adhering to its data protection principles without other formality), Dalkia will also ensure, in accordance with the recommendations of the European Data Protection Board relating to measures that complement transfer mechanisms intended to ensure compliance with the EU level of personal data protection, to assess the practical effectiveness of the chosen transfer mechanism with regard to the legislation of the third country. If it emerges from this analysis that the chosen transfer mechanism does not offer a level of protection essentially equivalent to that of the EU, Dalkia will

ensure, as far as possible, that additional measures (technical, organizational or contractual) are put in place and regularly evaluated.

7. What rights do you have over your personal data and how can you exercise them?

Under the conditions provided for by the applicable regulations, you have a right of access, rectification and opposition, a right of portability, erasure, limitation and the right to define guidelines relating to conservation. , the erasure and communication of your personal data after your death.

As a candidate who has been the subject of an exclusively automated decision to refuse following the use of a recruiter matching functionality, you also have the right to obtain human intervention from one of our recruitment managers so that they can review the decision, the right to express your point of view and to contest the decision that has been taken.

To find out more about the rights you have, you can consult the dedicated page of the National Commission for Information Technology and Liberties (CNIL):https://www.cnil.fr/fr/les-droits-pour-maitriser-vos-donnees-personnelles

You have the possibility to exercise your rights by contacting the data protection officer (“DPO”) of DALKIA SA:

- By post: DPO – Tour Europe – 33, place des corolles – TSA 77655 - 92099 Paris La Défense Cedex,
- Electronically:dpo@dalkia.fr

If, despite the response provided by Dalkia to your request, you are not satisfied, you have the possibility of submitting a complaint to the National Commission for Information Technology and Liberties (CNIL).

8. Review and update of our data protection policy

The content of this data protection policy is part of a dynamic review process for processing under Dalkia's responsibility, which is subject to regular updates.

Dalkia may therefore be required to modify this confidentiality policy in order to:

- To modify the list of treatments as well as their conditions of implementation
- To integrate regulatory and jurisprudential developments