1- PREAMBLE

As part of its activities, CIMPOR CAMEROUN S.A, and CIMPOR GIPSUM CAMEROUN, S.A. (hereinafter "CIMPOR" or "the company") as data controller, is required to collect personal data protected by **Law No. 2024/017 of December 23, 2024 on the protection of personal data in Cameroon**. The purpose of this Personal Data Protection Policy ***(hereinafter "the Policy")*** is to inform data subjects about the processing of their personal data collected and/or processed by the company, including during access to the company's website.

This Policy explains how CIMPOR collects, uses, stores and protects your personal data in accordance with Law No. 2024/017 of 23 December 2024 on the protection of personal data in Cameroon.

2- SCOPE

The Policy is intended to apply to all processing activities implemented by CIMPOR during which it is required to collect your personal data, including on the website accessible via the following address: https://www.cimporcameroun.com/fr (hereinafter the "Site") from which your data is also collected. CIMPOR has always included the protection of personal data as one of the major elements of its governance and the compliance of its procedures. This Policy applies to all data subjects whose personal data is processed by CIMPOR.

It shall be communicated to all Cimpor employees without distinction of level, in the most appropriate manner and in accordance with the standards in force. This Policy complies with the provisions of Law No. 2024/017 of December 23, 2024 on the protection of personal data in Cameroon. It can be supplemented as necessary by the general principles of law or the customary practice/international good practice.
This Policy is updated regularly and any substantial changes will be subject to prior communication.

3- DEFINITIONS

Accountability: refers to the obligation for companies to implement their own internal mechanisms and procedures for the protection of personal data and demonstrating that they are in compliance with the law on the protection of personal data.

Consent: any express, unequivocal, uncoerced and free and informed by clear, precise and complete information by which the data subject, or his or her legal representative, agrees to the processing of his or her personal data.

Data Controller: refers to the entity that carries out the processing of the personal data that it collects. CIMPOR is the data controller of the personal data it collects.

Data Processor: refers to any natural or legal person who processes personal data on behalf of the Data Controller and under its instructions.

Data subjects: any natural person whose personal data is processed.

Personal data: information relating to a person that allows him or her to be identified directly or indirectly, in particular by reference to any form of identifier or to one or more elements specific to his or her identity such as a name, an identification number, location data, an online identifier or to one or more specific elements specific to his or her physical identity, psychological, genetic, psychological, cultural, socio-professional or economic information, including a name, a photo, a fingerprint, a postal address, an email address, a telephone number, a social security number, an internal number, a numerical identifier, an IP address, a computer connection identifier, a voice recording.

Personal Data Protection Impact Assessment (DPIA): a procedure to analyse the likelihood and severity of risks to the rights and freedoms of Data subjects resulting from the processing of personal data.

Privacy by Design and Privacy by Default:

√ **Privacy by Design:** Means the taking into account the impacts on privacy from the design of the processing of personal data. It is characterised by proactive measures to anticipate and prevent adverse events data protection before they happen.

√ **Privacy by Default:** is the principle that the controller ensures that only the data that is strictly necessary for each specific purpose of the processing is processed by default without the user's intervention.

Processing: any operation or set of operations relating to personal data, irrespective of the process used, including collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or interconnection, and blocking, erasure or destruction.

Pseudonymization: a technique used to replace directly identifiable data with artificial identifiers in order to protect the privacy of individuals.

Recipients of the processing of personal data: natural or legal person, public authority or any other body authorised to receive communication of personal data, whether or not it is a third party.

Sensitive data: information relating in particular to religious, philosophical, political, trade union opinions and activities, banking transactions, racial or ethnic origin, linguistic, regional, sex life, genetics, biometrics, health, legal proceedings and criminal sanctions.

Standard contractual clauses: clauses in the model contracts drawn up and published by the personal data protection authority to provide a legal framework for any transfer of personal data between parties located on Cameroonian territory on the one hand and an actor located outside Cameroonian territory on the other hand, the content of which can only be modified to provide for greater protection of the personal data transferred.

4- DATA COLLECTED

Categories of data subjects	Categories of data processed
✓ Website Visitors ✓ Website users	**Identification data** **Professional data**
✓ Prospects ✓ Customers ✓ Business Partners ✓ Suppliers and Subcontractors ✓ External or occasional collaborators ✓ Candidates/Temporary Workers	**Identification data** *(e.g. surname, first name, contact details, photograph, etc.)* **Legal and tax information** (NIU, tax compliance certificate, bank details) **Professional data**
✓ Family ✓ Dependents or other persons in relation to CIMPOR employees	**Identification data** **Personal life data** *(e.g. family situation, etc.)* **Legal and tax information**

BQ.

✓ Employees and officers of CIMPOR or any of its subsidiaries; ✓ Retirees and people who have previously held positions within the company	**Identification data** **Personal life data** **Legal and tax information** **Data relating to professional life** *(e.g. registration number, training, diplomas, professional evaluation, data necessary for the appointment and operation of staff representative bodies or trade unions, etc.)*
✓ Employees ✓ Company Directors	**Identification data** **Personal life data** **Legal and tax information** **Data relating to professional life**
✓ Employees and Officers ✓ Business partners; ✓ Suppliers and Subcontractors;	**Economic and financial information** *(e.g. bank details for the payment of salaries, etc.)*
✓ Employees ✓ Company Directors	**Data necessary for the organization of work** *(e.g. directories and internal organizational charts, connection logs recorded to ensure the security and proper functioning of computer applications and networks, data from professional applications or tools)*
✓ Employees ✓ Company Directors	**Special data** *(e.g. social security number for social declarations)*
✓ Website users ✓ Employees ✓ Company Directors ✓ Prospects ✓ Customers	**Data made public by the data subjects** *(Example: profiles from professional social networks)*
✓ Website users ✓ Employees ✓ Company Directors ✓ Prospects ✓ Customers	**Login details**

5- THE RECIPIENTS OF THE DATA

In the context of CIMPOR's activities, third parties (such as subcontractors, lawyers, service providers or partners - such as mutual insurance companies, the National Social Insurance Fund, managers of employee savings accounts) may be recipients of or have access to some of the personal data of employees, external workers and occasional workers.

CIMPOR ensures that access to personal data is strictly limited to those who need access to it to perform their duties. CIMPOR implements access control procedures, such as clearance management, to ensure data security.

The recipients are:

a) CIMPOR and CIMPOR Service Providers

The personal data of employees, external and occasional workers may be communicated, when necessary, to line managers, reception staff, and other departments of CIMPOR to meet its legal, regulatory, or contractual obligations, for organisational, operational, administrative management, security reasons, and/or for reasons relating to the legitimate interest of the company.

Some of the personal data may also be transmitted:

- to the trade union organisations representing the staff for their trade union communication sent by internal mail, namely:
  - occupational data (entity, place of work, occupational category, etc.);
  - identification data (surname, first name, etc.).

- to the staff representative bodies in the context of the exercise of their missions and the management of social and cultural activities (in accordance with the agreements binding them to CIMPOR), namely:
  - of professional data;
  - identification data.

Data subjects may object to the transmission of their personal data at any time, from the date of their employment, unless transfer or their personal data is a processing activity required by law. Otherwise, this data will be transmitted to the employee representative organisations and bodies, however they may then object to it at any time also to the staff representative organisations and bodies concerned.

Refusal to transmit this personal data to the employee representative bodies will not have any negative impact on accessibility to the social and cultural activities organised by CIMPOR. The Data Subjects concerned can directly contact the representative bodies for any request related to these activities.

b) Third parties

As part of CIMPOR's usual activities, authorised third parties (such as subcontractors, consultants, service providers, partners, or mutual insurance companies, etc.) may be recipients of or have access to some of the personal data of employees, external and occasional collaborators, for example in the context of the performance of a contract.

In such a case, CIMPOR ensures that the transfers or exchanges are necessary for the performance of the tasks entrusted by CIMPOR and carried out within the limits of these purposes, providing all appropriate data protection guarantees.

Some of the personal data of employees, external and occasional collaborators may also be sent, in compliance with the applicable regulations, to third parties in Cameroon or abroad for the purpose of establishing, safeguarding or defending a legal right, in the context of administrative or criminal investigations by one or more regulators, the fulfilment of commitments made to them or in the context of legal disputes of any kind.

Some of the personal data of employees, external and occasional collaborators may thus be transmitted not only to regulators or judicial authorities but also to CIMPOR's counsel and those of the other parties to the lawsuit, as well as to these parties themselves.

In such a case, CIMPOR ensures that the data transferred or exchanged is relevant and necessary for the purposes referred to above.

BP.

Data Type	The recipients of the data
✓ Professional data (entity, place of work, professional category, etc.) ✓ Identification data (surname, first name, etc.)	Staff representative trade unions; Labour inspectorate
✓ Professional data (entity, place of work, occupational category, etc.) ✓ Identification data (surname, first name, etc.)	Subcontractors, lawyers, service providers or partners

6- PRINCIPLES APPLICABLE TO PERSONAL DATA

CIMPOR is committed to compliance with the principles provided for by Law No. 2024/017 of December 23, 2024 on the protection of personal data in Cameroon.

6-a Principle of finality

The personal data collected by CIMPOR may only be processed for the purpose indicated at the time of collection, which arises from the circumstances, or which is provided for by law, and is only for purposes that are specified, explicit and legitimate to its activity.

Personal data is collected for specified, explicit and legitimate purposes, and processed in a fair and transparent manner. The data is not subsequently used for other purposes in a manner that is incompatible with its purposes.

6-b Relevance, adequacy and minimization of the data collected

Only strictly necessary data is collected and processed in accordance with the principle of minimization.

6-c Accuracy

In the context of the processing of personal data, CIMPOR ensures that it is accurate. This term also means that only personal data that is adequate, relevant and strictly necessary with regard to the purposes of the processing are collected and processed.

6-d Data Security

The data controller implements security measures for the premises and information systems, to prevent unauthorised access to the data, which is reserved only for persons designated and authorised by virtue of their position.

6-e Lawfulness of the processing implemented

The processing of personal data by CIMPOR may only take place if according to a lawful basis. CIMPOR guarantees that the data is not misused or for purposes other than those for which it was collected and is not subject to any act of unauthorized modification or deletion of the data. CIMPOR ensures the lawfulness and probity of the content of personal data conveyed by its communications network, in particular when such content is able to violate human dignity, honour and privacy.

6- f Good faith

Each processing of personal data by CIMPOR is subject to prior, clear and transparent information to the data

in the forms, on the rights they have and on the terms and conditions for the effective exercise of these rights. In addition, each processing carried out is accompanied by information notices. No collection is carried out without the knowledge of the Data Subjects or against their will, whenever consent is required.

7- THE PURPOSES OF THE PROCESSING

The personal data collected may be used for the following purposes:

7-1-a Regarding human resources management:

- Administrative management of employees (recruitment file, professional file, statistics, list of employees, directories, organisation chart, provision of professional equipment, management of working time (teleworking, on-call duty, etc.), management of absences and leave, management of departures, etc.);
- The provision of IT tools (monitoring and maintenance of equipment, IT directories, application and network security devices, e-mail, intranet, etc.)
- Work organization (task and schedule management, etc.);
- Career management (assessment, performance evaluation, management of professional skills, validation of prior learning, mobility, etc.);
- Employee training;
- Management of internal communication (social networks, events, seminars, various communications such as newsletters, etc.);
- Compliance with internal policies and procedures, investigation and disciplinary actions.

7-1-b The management of social relations and in particular for:

- The functioning of staff representative bodies and representative trade union organisations (management of social and cultural activities, trade union communication, production of social reports, etc.);
- The organisation of the elections of staff representatives;

7-1-c Compensation management:

- The calculation and payment of remuneration and accessories and professional expenses;
- Carrying out operations resulting from legal provisions, collective agreements or contractual stipulations concerning declarations to the tax authorities and the national social security fund,
- The keeping of individual accounts relating to employee profit-sharing and profit-sharing, etc.;
- The provision of information and the preparation of reports on the situation of personnel in order to comply with legal obligations (keeping the single personnel register and the declaration of employment of disabled workers, etc.);

7-1-d Access control management:

- Access control at the entrance (entry badges) and in certain premises subject to a traffic restriction;
- Restaurant access control and associated payment;
- Visitor access control
- Video surveillance cameras, drones or other similar equipment

7-1-e Geolocation management

- The safety or security of the employee himself, the goods, the vehicles in his care and the optimization of resources.
- The better allocation of resources for services to be performed in dispersed places, in particular for emergency interventions.

BP.

7-2 Regarding maintenance:

- Maintenance contract management
- Authentication of maintenance workers
- Management of access and authorisations for maintenance workers
- Recording and logging of equipment maintenance interventions
- Establishment of maintenance vouchers
- Management of data provided by hardware

7-3 Regarding the management of the relationship with customers and the purchasing department

- Advertising call management
- Newsletter management
- Customer database management
- Subscription management and loyalty card issuance
- Invoicing
- Purchase history management
- The management of unpaid bills
- Keeping customer files
- Collecting contact information from prospects via questionnaires
- Drawing up delivery notes, issuing invoices
- Managing and updating the supplier roster
- Customer complaints

7-4 Concerning logistics and supply management

- Supplier data management
- Purchase order management
- Management of incoming goods vouchers
- Management of delivery notes to customers
- Management of goods transfer orders between warehouses

7-5 Concerning suppliers and service providers:

- Management of the administrative file (identification, start date of the contract, end date, etc.);
- Compensation management if applicable (internship bonuses for interns);
- Access control at the entrance (entrance badge);
- Restaurant access control and associated payment if applicable
- The provision of IT tools (monitoring and maintenance of equipment, possibly computer directories, application and network security devices, electronic messaging, intranet, etc.).

7-6 Regarding project management:

- Establishment of project charters
- Drafting of management plans
- Drafting statements of work
- Drafting and maintaining Risk Registers
- Writing and keeping problem and difficulty logs
- Writing and maintaining project status reports
- Drafting and keeping minutes of meetings

7-7 Concerning all the persons concerned:

- Managing the protection and security of affected persons, CIMPOR's activities and assets;
- Management of the organization's steering, reporting and control missions *(e.g. risk management and mitigation);*

- Managing and organizing compliance with CIMPOR's legal, regulatory, conventional or compliance obligations (*e.g. the implementation of internal control procedures or alert mechanisms*);
- Litigation management;
- The reconciliation of some of the personal data of the data subjects with those present within the customer base of the CIMPOR network, with a view to verifying the status of the employee or worker, for the purposes of complying with CIMPOR's obligations in regulatory and contractual matters, or for reasons relating to the legitimate interest of the company.

Specific processing may be implemented in the context of the use of certain applications. In these cases, the specificities relating to the protection of personal data will be specified.

8- THE LEGAL BASES FOR THE PROCESSING IMPLEMENTED BY CIMPOR

Any processing implemented by CIMPOR is based on the following legal bases.

8-1 The consent of the person concerned:

Personal data is collected and processed with the explicit consent of the data subjects when required by law, in particular for:

- ✓ Processing of sensitive data;
- ✓ The management of social and cultural activities;
- ✓ Internal communication via newsletters or social networks;
- ✓ Communicating personal data to third parties or using them on their behalf for direct marketing purposes;
- ✓ Any use not directly related to a legal or contractual obligation.

Consent must be free, specific, informed and unambiguous. CIMPOR puts in place mechanisms to collect consent in an express manner and to retain proof of consent. Data subjects have the right to withdraw their consent at any time (see Section 12 of this Policy and the Documentation of Procedures for the Protection of the Rights of Data Subjects).

8-2 Performance of the contract or pre-contractual measures

The contract is one of the legal basis provided by the Personal Data Protection Act on which the processing of personal data may be based. The use of this legal basis assumes that the processing is objectively necessary for the performance of a contract between CIMPOR and the data subject (*management of requests and complaints, performance of an employment contract, etc.*).

The data necessary for the performance of contracts executed with our employees, service providers or partners are processed in the following context:

- ✓ Administrative management of employees (HR files, organizational charts);
- ✓ Payment of remuneration/fees and accessories;
- ✓ Provision of professional IT tools.

8-3 Legal and regulatory obligations

Some data is processed to meet our regulatory and legal obligations, including:

- ✓ Tax and social declarations;
- ✓ Keeping of accounts relating to profit-sharing;
- ✓ Transmission to the competent authorities in the context of judicial or administrative investigations;

Regulatory compliance obligations.

8-4 CIMPOR's legitimate interests

CIMPOR may process certain data to pursue its legitimate interests while respecting the fundamental rights of data subjects. These processing include:

BP.

- ✓ Internal organization and operational management;
- ✓ Advocacy at the administrative and judicial levels;
- ✓ Securing information systems, assets and people;
- ✓ Assessment and management of internal professional skills.

Prior to any processing based on consent or legitimate interest, CIMPOR undertakes to provide clear and detailed information to data subjects regarding:

- ✓ The purposes of the processing;
- ✓ The applicable legal basis;
- ✓ The rights they have.

Data subjects may request clarification at any time on the legal basis applicable to their personal data by contacting our Data Protection Officer (DPO) at the following address: (dpocimpor@cimpor.com)

8-5 A mission of public interest

The processing may be necessary for the performance of a task carried out in the public interest.

8-6 Safeguarding vital interests

The protection of the vital interests of the data subject, or of a third party, may justify the processing of personal data by CIMPOR.

9 - CIMPOR'S SUBCONTRACTORS

CIMPOR's service providers may be required to process personal data on behalf of CIMPOR. To this end, CIMPOR chooses its subcontractors carefully and requires them to:

- adopt a level of protection of personal data equivalent to its own, a use of personal data or information only to ensure the management of the services they must provide;
- strict compliance with the applicable legislation and regulations on confidentiality, banking secrecy, business secrecy and the protection of personal data;
- the implementation of all appropriate measures to ensure the protection of the personal data they may be required to process;
- the definition of the technical and organisational measures necessary to ensure security;

CIMPOR has executed contracts with its subcontractors, in accordance with legal obligations, that provide for obligations with regard to the protection of personal data and ensures that its subcontractors provide sufficient guarantees as to the implementation of appropriate technical and organisational measures. In particular, they must:

- Implement measures to ensure data protection;
- Use the data in strict accordance with CIMPOR's instructions;
- Notify immediately in the event of a security incident;

10- Limitation of the retention period

In accordance with Article 13 of Law No. 2024/017 of December 23, 2024 on the protection of personal data in Cameroon, CIMPOR retains personal data only for the time strictly necessary to achieve the purposes for which they were collected. Once this period has expired, the data is deleted or anonymised, unless there is a legal or regulatory obligation requiring it to be kept for a longer period.

10-1 Specific durations according to the purposes

BP

The retention periods applicable to the different categories of data processed by CIMPOR are as follows:

- The personal data of the persons concerned are kept for the purposes announced, in compliance with the legal requirements in force, in particular in civil, tax, commercial and criminal matters.
- Data for the purpose of managing recruitment are kept, unless otherwise requested, **for two years** from their receipt or the last contact with the candidate.
- Data for the purpose of personnel management are kept **for the duration of the employee's contract**. Some data may be kept beyond that, but always within the legal deadlines in force in the regulations.
- Customer data used for commercial prospecting purposes is kept during the commercial relationship, then for **a period of three years** from the end of the commercial relationship (for example, from the date of a purchase, the expiry date of a warranty, the end of a service contract or the last contact from the customer).
- Personal data relating to a non-customer prospect may be kept for a **period of three years** from the date of collection by the data controller or the last contact from the prospect
- Finally, the collection of proof of identity in the context of the exercise of rights is only possible when there is a reasonable doubt as to the identity of the person.
- However, it is possible to keep these documents for evidentiary purposes in certain exceptional cases where the data controller identifies a strong litigation risk, according to a case-by-case and duly documented analysis. In this case, the period of retention of the supporting documents is determined in accordance with the limitation periods for prosecution provided for in the provisions of Article 65 of the Code of Criminal Procedure, without prejudice to interruptive acts, legal or factual obstacles that prevent the initiation of public proceedings:
    - by **ten years** from the day after the day on which the crime was committed
    - In the case of misdemeanour, subject to the provisions specific to certain offences, **three years**
    - In the case of contraventions, the statute of limitations for public prosecution is **one year**
- Data for the purpose of geolocation are kept in principle for a **period of two months**.
- It may be kept for a **period of one year** for the purpose of proving the performance of a service, when it is not possible to provide such proof by any other means.
- It can be kept for **up to one year** to keep a history of movements for route optimization purposes.
- It can be kept for a **period of five years** as part of the monitoring of working time, only the data relating to the hours worked.

10-2 Records Management

The personal data processed is kept in the form of archives by CIMPOR, distinguishing:

✓ **Current archives correspond to active data:** their retention period corresponds to the intended purpose of the processing.

✓ **Intermediate archives:** these are documents which, no longer considered as current archives, cannot yet be disposed of or definitively preserved, because of their administrative interest or their episodic usefulness, their conservation is mandatory for legal reasons, and the retention periods are regulated. Access to the personal data stored in this context is strictly limited to a service with access rights and authorisations.

CIMPOR has set up a mechanism for isolating archived data by means of a specific separation. At the end of the retention period, the personal data will be destroyed or anonymised so that it is no longer possible to identify the persons concerned.

✓ **Definitive archives**: these correspond to documents which, at the end of routine or episodic use, are kept because of their historical or statistical interest justifying that they are not subject to any destruction.

They are kept on an independent medium, not accessible by the production systems, allowing only separate, punctual and precisely justified access to the company's archives department, which is the only one authorised to consult this type of archive. It is also anonymised so that it is no longer possible to identify the persons concerned.

CIMPOR implements an archive management policy to ensure the retention and security of personal data in accordance with the legal and regulatory requirements in force. This policy includes:

- ✓ Defining the personal data lifecycle;
- ✓ The definition of the retention periods applicable to each cycle;
- ✓ The implementation of appropriate security measures to protect archived data against unauthorized access, accidental loss or destruction;
- ✓ Defining the terms and conditions of access to archived data;
- ✓ The implementation of procedures for the destruction or anonymization of data at the end of the cycle.

11 - TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES AND THE TRANSFER MECHANISMS IMPLEMENTED

With regard to the structuring of the group and CIMPOR's activities, personal data may be transferred to countries outside Cameroon under the following conditions:

- ✓ The transfer is necessary for the performance of a contract or a pre-contractual act to which the data subject is a party.
- ✓ CIMPOR and its international branches have issued and submitted to the control and validation of the competent Protection Authority of Binding Corporate Rules;
- ✓ The recipient country benefits from an adequacy decision by the competent authority;
- ✓ The Competent Authority has authorized the transfer in view of the existence in the recipient country of equivalent mechanisms for the protection of personal data (Art. 32 of the Cameroonian Data Protection Law);
- ✓ Approved standard contractual clauses are implemented to ensure equivalent protection;
- ✓ Additional safeguards (encryption, anonymization) are applied when necessary.

With this in mind, CIMPOR refers the matter to the personal data protection authority in order to obtain authorisation, in accordance with the regulations in force, to guarantee the exercise of the rights of the data subject. To this end, the company will make available to the data subject and to that of the authority in charge of the protection of personal data in Cameroon;

- ✓ The summary of the transfers of personal data envisaged and the transfer mechanism chosen for each;
- ✓ Documentation relating to the implementation of transfers according to the chosen mechanism;
- ✓ Adequacy decisions;
- ✓ The legal instrument signed with the country of destination;
- ✓ The Standard Contractual Clauses for the protection of personal data signed with importers and exporters of personal data;
- ✓ Binding Corporate rules and their approval decision;
- ✓ Documents relating to the transfers made, such as proof of the data subject's consent or the balancing analysis of the interests of the data subject and the Data Controller;

12- RECOGNIZED RIGHTS

12-a The right of access to data

CIMPOR gives data subjects confirmation as to whether or not their personal data is being processed and where it is, they have the right to request a copy of their data and information regarding:

- The purposes of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipients and, where applicable, if such communication is to be made, the bodies to which the personal data have been or will be disclosed, in particular recipients who are established in third countries;
- Where possible, the envisaged retention period of personal data or, where this is not possible, the criteria used to determine this period;
- The existence of the right to request from the controller the rectification or erasure of their personal data, the right to request a restriction of the processing of their personal data, the right to object to such processing;
- The right to lodge a complaint with a supervisory authority;
- Information about the source of the data when it is not collected directly from the data subjects;
- The existence of automated decision-making, including profiling, and in the latter case, useful information regarding the underlying logic, as well as the significance and expected consequences of such processing for data subjects.

12-b The right to rectification of data

CIMPOR recognises the right of data subjects concerned to request that their personal data be rectified or completed, as the case may be, if they are inaccurate, incomplete, ambiguous or outdated.

12-c The right to erasure of data

CIMPOR recognises the right of data subjects to request the erasure of their personal data on one of the following grounds:

- ✓ Personal data is no longer necessary in relation to the purposes for which it was processed;
- ✓ The consent on which the processing is based is vitiated; they have decided to withdraw the consent previously given;
- ✓ Consent has expired;
- ✓ The processing carried out does not have a legal basis;
- ✓ Any other reason provided for by law.

The attention of the data subjects is drawn to the fact that the right to erasure of data is not a general right and that it can only be granted if one of the grounds provided for in the applicable regulations is present.

If none of these reasons are present, CIMPOR will not be able to respond favourably to such a request; This will be the case if the company is obliged to retain the data due to a legal or regulatory obligation or for the establishment, exercise or defence of legal claims.

12-d The right to restriction of processing

CIMPOR recognizes the right of data subjects to request the limitation of the processing of their personal data in the cases provided for by Law No. 2024/017 of December 23, 2024 on the protection of personal data in Cameroon, in particular when the accuracy of the personal data, or the purpose is disputed.

If the processing has been restricted by virtue of the exercise of this right, the data may only be processed with the consent of the data subject or for the establishment, exercise or defence of legal claims, or for the protection of the rights of another natural or legal person.

12-e The right to object to data processing

CIMPOR recognises the right of the data subjects to object to data processing at any time, for:

- Any reasons relating to the processing of special categories of personal data;
- Any processing for canvassing purposes;
- Any reason provided for by law.

In the event of exercising such a right to object, CIMPOR ensures that it no longer processes the personal data in question in the context of the processing in question unless CIMPOR may have compelling legitimate grounds for maintaining such processing or justifying grounds for establishing, exercising or defending legal claims of a legitimate or vital interest that outweigh the rights and freedoms of the data subject.

12-f The right to data portability

CIMPOR recognizes the right of data subjects to the portability of their personal data. This right only applies to automated processing, excluding manual or paper processing.
This right is limited to processing operations whose legal basis is consent or the performance of pre-contractual measures or a contract.
This right does not include derived data or inferred data, which are personal data created by CIMPOR.

The data on which this right can be exercised are only current personal data, which excludes anonymised personal data or data that does not concern the applicant.
The right to portability may not infringe on the rights and freedoms of third parties such as those protected by trade secrets.

CIMPOR recognises the right of data subjects to request data portability with the possibility of receiving the data themselves or, if technically feasible, the direct transmission of the data by CIMPOR to another data controller. In the latter case, CIMPOR asks the data subjects to indicate the exact name of this data controller, their contact details and the department or person who should be the recipient. In order to facilitate the exercise of this right, the person concerned must inform the recipient of the request to the services of CIMPOR.

12- g The right to withdraw consent

When the data processing that CIMPOR implements is based on consent, the data subject may withdraw it at any time. CIMPOR then ceases to process the said personal data, without this calling into question the lawfulness of the processing carried out before this withdrawal.

12-h Right not to be subject to a decision based solely on automated processing

CIMPOR recognises the right of data subjects not to be subject to a decision based exclusively on automated processing, including profiling, producing legal effects concerning them, unless this decision is necessary for the conclusion or performance of a contract, is permitted by law or is based on their explicit consent.

12-i Right to object to the disclosure of personal data to third parties

CIMPOR recognizes the right of data subjects to object to the disclosure of their personal data to third parties, in accordance with the provisions of Law No. 2024/017 of December 23, 2024 on the protection of personal data in Cameroon. This right may be exercised in particular when the data subject has legitimate reasons to believe that such disclosure may infringe upon their privacy, freedoms, or fundamental rights.

Unless otherwise provided by law or justified by a legitimate and overriding interest, no personal data shall be disclosed to a third party without the data subject's prior consent. Where the right to object is exercised, CIMPOR shall refrain from communicating the data to the third party concerned, unless such communication is necessary for legal compliance, the establishment, exercise or defence of legal claims, or the protection of the vital interests of the data subject or another person.

12-j Right to prior information in case of processing for commercial prospecting purposes

CIMPOR recognizes the right of data subjects to be informed in advance of any processing of their personal data for commercial prospecting purposes, in accordance with the provisions of Law No. 2024/017 of December 23, 2024 on the protection of personal data in Cameroon. This information must be clear, accessible, and must include, in particular, the identity of the data controller, the intended purposes of the prospecting, the nature of the data used, and the rights granted to the data subject, especially the right to object at any time to such processing.

No commercial prospecting activity shall be carried out by CIMPOR without the data subject having been expressly informed beforehand and, where applicable, given the opportunity to exercise their right to object.

12- k The right to issue post-mortem directives

CIMPOR recognizes the possibility for data subjects to define specific directives relating to the storage, deletion and communication of their personal data after death, to its services in accordance with the terms defined by Law No. 2024/017 of December 23, 2024 on the protection of personal data in Cameroon. These special guidelines will only concern the processing implemented by CIMPOR and its subcontractors.

12 - l The right to lodge a complaint

Data subjects have the right to lodge a complaint relating to the exercise of their rights with CIMPOR or the authority in charge of the protection of personal data in Cameroon without prejudice to any other administrative or judicial remedy, in accordance with the relevant provisions in this matter and in accordance with the cases provided for by law.

To exercise any of these rights with CIMPOR, the persons concerned must send their requests in writing, providing proof of their identity, to the following address:

- By email: dpocimpor@cimpor.com
- By post: (PK3+700 Rond-Point Autoroutier Kribi-Lolabe of CIMPOR's head office, for the attention of the department concerned).

CIMPOR undertakes to respond within a maximum of 30 days from receipt of the request. In the event of refusal or incompleteness, a justification will be provided to the person concerned.

For more detailed information on how to exercise rights and how CIMPOR handles requests for these rights, please consult our **Policy for the Management of Requests for the Exercise of Rights**, available on the company's website accessible through the following link: [link to the policy] or on request from customer service.

13- CONNECTION TO SOCIAL NETWORKS

On the Site https://cimporcameroun.com/fr the connection to social networks is effective thanks to the tabs provided for this purpose. If the user decides to connect to social networks from the Site, CIMPOR draws his attention to the fact that he communicates the information of his profile according to the social network settings used. CIMPOR invites users to visit the social network concerned and consult its personal data protection policy in order to understand how their data is shared and used in this context.

14- COOKIE MANAGEMENT

The Website uses "cookies" which are trackers of navigation on a website, read or deposited. Thus, the Site is likely to enter information into the user's equipment or electronic communications terminal and to access information that is already stored there. The trackers used by the site fall into two categories:

- Trackers that are exempt from the user's prior consent, and
- Other trackers subject to the prior consent of the user.

In accordance with the applicable regulations on personal data, CIMPOR informs about the purpose of the cookies used, the methods made available and the possibilities of objecting to them.
For more detailed information on how CIMPOR processes cookies, please see our **Cookie Policy** available on the company's website at the following address: [link to the cookie policy on the website]

15- GOVERNANCE OF PERSONAL DATA AND COMPLIANCE WITH THE PRINCIPLE OF ACCOUNTABILITY BY CIMPOR

CIMPOR fully recognizes its status as a data controller and has implemented internal mechanisms and procedures to demonstrate at all times and on an ongoing basis compliance with the rules imposed by the law on the protection of personal data, in particular through the implementation of technical and organizational measures on the one hand and on the other hand compliance with an obligation to provide documentation guaranteeing the security of the processing carried out on the personal data in order to prevent any breach thereof.
A breach of security resulting in, accidentally or unlawfully, the destruction, loss, alteration, unauthorized disclosure or use of, or access to, personal data transmitted, stored or otherwise processed, constitutes a personal data breach within the meaning of the Personal Data Act in Cameroon.
To this end, CIMPOR takes appropriate technical and organisational measures to guarantee a level of security appropriate to the risks presented by the processing implemented. These measures are reviewed and updated as necessary. They concern the demonstration of the existence of *accountability* and the documentation of *accountability*.

15-1 Demonstration of the existence of *accountability*

It covers compliance with the principles relating to the processing of personal data, **the security of personal data,** compliance with the requirements of *Privacy by Design* and *Privacy by Default*.

15-1-a Compliance with the principles relating to the processing of personal data

CIMPOR can thus demonstrate compliance with the principles relating to the processing of personal data such as:

a) Lawfulness, fairness and transparency of processing;
b) Purpose limitation;
c) Minimization;
d) Accuracy of personal data;
e) Limitation of the retention period;
f) Integrity and confidentiality of personal data.
g) End-to-end security - full lifecycle protection.

15-1-b Security of personal data

CIMPOR has developed an Information Systems Security Policy (ISSP) to ensure the security of infrastructures, resources and application systems.
Our websites use various security measures. Authentication tools are encrypted to ensure the security of your personal data.
CIMPOR has implemented procedural and technical safeguards in accordance with legal requirements and the current state of the art, at each stage of the processing of personal data.
These measures are designed to protect against the unlawful destruction, loss, alteration, use, disclosure, or unauthorized access to personal information. To these ends, CIMPOR has implemented the following technical and organizational security measures in order to guarantee a level of security appropriate to the risks associated with the processing:

✓ Raise awareness and authenticate users;
✓ Manage authorisations;
✓ Trace access and manage incidents;

- ✓ Secure workstations and mobile computing;
- ✓ Protect the internal computer network;
- ✓ Secure the servers and the website;
- ✓ Safeguarding and planning for business continuity;
- ✓ Archive securely;
- ✓ Supervise the maintenance and destruction of data;
- ✓ Manage subcontracting
- ✓ Secure exchanges with other organizations;
- ✓ Protect the premises;
- ✓ Supervise IT developments;
- ✓ Encrypt and ensure integrity.

15-1-c Compliance with the requirements of *Privacy by Design* and *Privacy by Default*

The concept of *Privacy by Design* within CIMPOR means that data protection requirements are taken into account as early as possible from the design stage. In other words, data protection aims to integrate data protection and privacy into the design of processing activities and information systems, in order to comply with data protection principles.

The concept of *Privacy by Default* is the principle that the controller ensures that only the data that is strictly necessary for each specific purpose of the processing is processed by default without the intervention of the user.

15-1- d Technical and organizational measures under *Privacy by Design*

Data protection by design aims to integrate data protection and privacy into the design of processing activities and the security of information systems, in order to comply with data protection principles. To meet the requirements of the law, CIMPOR has implemented the following measures regarding personal data.

They relate to:

- ✓ Pseudonymization systematically applied to sensitive data;
- ✓ Ensuring transparency as to purposes and processing;
- ✓ The presence of information;
- ✓ The presence of charters;
- ✓ The possibility given to the data subject to control the processing of his or her personal data;
- ✓ The implementation of security measures;
- ✓ Encryption of confidential data;
- ✓ The management of access rights;
- ✓ Tools to combat external intrusions into the network (firewall, anti-virus);
- ✓ Password Policy;
- ✓ Replacing direct identifiers with secure, separately stored alphanumeric codes;
- ✓ Protection via secure flows;
- ✓ AES-256 encryption for storing and transferring sensitive data;
- ✓ Multi-factor authentication to limit access to systems;
- ✓ Regular audits to verify compliance with ISO/IEC 27001 standards;
- ✓ The existence of a data mapping procedure;
- ✓ Review of contracts (subcontractors, partners, employees, customers)
- ✓ Awareness/training of business and IT teams;
- ✓ Keeping a register of processing activities;
- ✓ Risk analysis (DPIA);
- ✓ The management of people's rights.

15-1-e Technical and organisational measures under *Privacy by Default*

CIMPOR implements appropriate technical and organizational measures to ensure the data minimization policy so that by default, only necessary personal data is processed. This concerns:

- ✓ The reduction of their treatment to a minimum
- ✓ The amount of personal data collected;
- ✓ The extent of their treatment;
- ✓ Their retention period shelf life;
- ✓ Their accessibility.

The measures described above ensure by default that personal data is not made accessible to an unknown number of people, without the consent of the data subject.

15-1-f Data Breach Management

In the event of a personal data breach that may pose a risk to data subjects, CIMPOR will:

- notify the Data Protection Authority within 72 hours;
- inform affected persons if the risk is high, specifying the nature of the breach and corrective actions;
- diligently take measures to strengthen security arrangements and prevent recurrence.

A register of data breaches shall be kept up to date and accessible to the competent authority in the event of an audit.

15-2. ACCOUNTABILITY DOCUMENTATION

Concerned about the importance of the protection of personal data, CIMPOR has put in place all the documentation elements to demonstrate its compliance with the law on the protection of personal data at all times to the competent authorities. This documentation is updated regularly and includes:

15-2-a Internal procedures relating to *Privacy by Design, Privacy by Default* and Privacy Impact Assessments, including:

- ✓ Documentation to demonstrate the consideration of personal data protection in the context of the implementation of new products
- ✓ The impact assessments carried out, including their updates.

15-2- b Documents concerning the appointment of a Data Protection Officer (DPO) and his or her appointment

- ✓ The DPO's mission letter;
- ✓ The professional qualifications of the DPO
- ✓ Guarantees of the DPO's independence

15-2-c Documentation relating to the personal data protection policy

- CIMPOR's Personal Data Privacy Policy
- CIMPOR's personal data retention policy
- Documentation of the procedures implemented to ensure respect for the rights of data subjects;
- The templates for the main information and consent clauses contained in the contracts, on the website and other main channels of communication with CIMPOR data subjects;
- Documentation relating to the management of data subjects' requests, including requests to exercise their rights and responses provided by CIMPOR;

- Documentation relating to the mechanism implemented by CIMPOR to ensure the traceability and monitoring of the rights exercised by the data subjects;
- Documentation relating to video surveillance.

15-2- d Documentation relating to contractual relations with Subcontractors

- Contracts with subcontractors;
- The monitoring policy governing subcontracting relationships (sample questionnaires regularly sent to subcontractors and responses to these questionnaires);
- The methods of auditing subcontractors;
- The results of the audits carried out and the actions taken as a result;

15-2-e Security Policy Documentation

- The information systems security policy and documentation describing the measures taken to ensure the security of personal data (pseudonymisation and encryption);
- The means to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The means to restore the availability of and access to personal data in an appropriate time frame in the event of a physical or technical incident.
- Test plans to regularly test, analyse and evaluate the effectiveness of the technical and organizational measures to ensure the security of the processing and the results of the security tests performed;
- The policy for the management of authorisations and access.

15-2-f Documentation relating to personal data breaches

- The internal policy on personal data breaches and contact details;
- The register of personal data breaches and notifications to data subjects and the authority in charge of the protection of personal data in Cameroon.

15-2 -g Processing Registers

All processing operations are listed in the Processing Register. As such, and depending on its roles, CIMPOR maintains several registers:

- A Data Controller Processing Register, where processing based on the consent of the data subject is separated from processing based on other legal bases;
- A Personal Data Breach Notification Processing Register.

Record-keeping is dynamic, updating as existing treatments evolve (including their removal) as well as new processing are created.

15 – 2-h Codes of conduct and certification:

- The document attesting to the existence of and adherence to a code of conduct and the associated documentation;

For more detailed information on our data governance commitments, please contact our DPO at email@example.com

16- UPDATE OF THE PERSONAL DATA PROTECTION POLICY

CIMPOR may modify this Policy in particular in order to take into account the evolution of the regulations applicable to personal data as well as any other regulations, in particular:

- The evolution of case law;
- The decisions of the authority in charge of the protection of personal data in Cameroon;
- The applicable regulations on the protection of personal data

The modification of this Personal Data Protection Policy is preceded by information to the persons concerned at least 15 days before.

The persons concerned shall be given this period to make observations, if necessary, on the new personal data policy. If no challenge is made within this period, the policy will be deemed accepted.

Kribi, the 23rd September 2025

CIMPOR CAMEROUN S.A.
The Country Director

CIMPOR CAMEROUN S.A
CIMPOR
NIU: M121712670072Q
PK3+700, Rond-Point Autoroutier Kribi - Lolabé

CIMPOR GYPSUM CAMEROON S.A.
The General Manager

CIMPOR GYPSUM CAMEROON
CIMPOR
GYPSUM CAMEROON
NIU: M072416990230
PK3+700 Rond-Point Autoroutier Kribi-Lolabe