PERSONAL DATA PROTECTION POLICY

1. INTRODUCTION

Since 25 May 2018, Regulation no. 2016/679, called the "General Data Protection Regulation" (or "GDPR"), has formed the new European legal framework, unique and common to all Member States, concerning the automated processing in whole or in part as well as the non-automated processing of personal data.

This regulation also has an extraterritorial context that, under certain conditions, allows its scope of application to be extended outside the EU.

The OPTORG Company has always considered the protection of personal data to be a key element of its governance and its operational, support and management processes and procedures.

2. INTERNAL CONTEXT

Depending on the situation, the Optorg Group takes on the role of Data Controller or Subcontractor.

Since these different qualifications result in distinct obligations and issues, this Data Protection Policy (hereinafter referred to as the "DPP") reflects the desire of the OPTORG Group to put in place all the principles applicable to the personal data collected and processed during its activities.

The OPTORG Group is attentive to its permanent respect for the following:

- The guidelines and directives of the Data Protection Act of 6 January 1978 as amended (the last amendment was formalised by Law No. 2018-493 of 20 June 2018, promulgated on 21 June 2018 to exercise some of the "national room for manoeuvre" allowed by the GDPR and transpose the Police-Justice Directive into French law);
- The guidelines and directives of the laws relating to the protection of personal data in the countries where its different subsidiaries are located.

3. DEFINITIONS

- **Personal data (hereinafter PD):** "Personal data means any information relating to an identified natural person or a person who can be identified, directly or indirectly, with reference to an identification number or to one or more items specific to the person...";
- **Processing**: any operation or set of operations involving such data, regardless of the process used, including the collection, recording, organisation, preservation, adaptation or modification, extraction, consultation, use, communication by transmission, broadcasting or any other form of provision, reconciliation or interconnection, as well as locking, deletion or destruction;
- **Data Controller**: the natural or legal person who determines the purposes and means of the processing of personal data. In general, the OPTORG Group is the Data Controller of its own data collections. However, in some cases, it may be that its customers are responsible for the processing;

- **Subcontractor**: any natural or legal person who processes personal data on behalf of the Data Controller. The OPTORG Group is the Subcontractor for the data it processes on behalf of its customers;
- **Subsequent Subcontractors**: the service providers of the Subcontractors with which the OPTORG Group works and who act on the personal data processed by the OPTORG Group as the Data Controller;
- **Data Subjects**: persons who can be identified directly or indirectly;
- **Data Recipients**: the natural or legal persons who receive the communication of personal data. The recipients of the data can therefore be internal recipients or external organisations.

4. SCOPE

The OPTORG Group has defined the principles and guidelines of this PPDC in order to:

1. Supervise, according to the GDPR, the processing of all collected data, regardless of how it is collected or processed;
2. Meet the obligation to inform the persons of their rights in a concise, transparent, understandable and accessible manner;
3. Formalise the rights and obligations of the OPTORG Group as the Data Controller and Subcontractor.

The OPTORG Group applies this DPP to all its subsidiaries, even those established outside of the EU, from the moment when they perform data processing:

- Relating to persons located in the European Union;
- Related to the supply of goods or services to such persons, whether or not payment is required.

CRITERIA FOR APPLYING THE EXTRA-TERRITORIAL FIELD OF THE GDPR

The following do not constitute an offer of goods or services to persons located in the European Union:

1. The simple accessibility from the European Union of the OPTORG Group's website, an e-mail address or other contact details;
2. The use of a language generally used in third countries where the Data Controller is established.

The following are considered to be evidence allowing the identification of an offer of goods or services to persons located in the European Union:

1. The use of a language or currency commonly used in one or more Member States of the European Union;
2. The option to order goods and services in that other language;
3. The mention of customers or users who are located in the European Union.

5. ACTORS INVOLVED IN IMPLEMENTING GDPR COMPLIANCE

To manage and boost the compliance of all of its entities with the regulations applicable to personal data, the OPTORG Group has appointed a Data Protection Officer (DPO) and has established a network of correspondents called Operational Data Controllers (ODCs).

5.1. DATA PROTECTION OFFICER (DPO)

The OPTORG Group has appointed a DPO with CNIL (Designation no. DPO-52428).

The DPO reports to the Legal and Fiscal Department. To ensure good compliance management, it also interacts with the ODCs, IT Services Department, Compliance Department and Human Resources Department.

Its main tasks are:

1. To inform and advise the OPTORG Group (management, staff involved in processing operations, etc.) on the rules that must be respected concerning the protection of personal data;
2. To monitor compliance with the rules for protection of personal data, including division of responsibilities, awareness raising and training of staff involved in processing operations and related audits;
3. To provide advice on request concerning PD impact analysis and to verify the implementation of PD;
4. To co-operate with the Supervisory Authority and act as the primary contact point for all matters regarding the processing of PD;
5. To ensure that the documentation of PD processing is maintained appropriately;
6. To ensure the maintenance of its skills by keeping informed of new developments in personal data protection.

The OPTORG Group ensures that the DPO is registered in the PSSI (as defined below) and is associated in an appropriate and timely manner with all matters regarding personal data protection, such as:

1. Privacy by Design, i.e. taking account of privacy impacts from the design stage of PD processing;
2. Privacy by Default, i.e. taking account of the impact on data protection by default;
3. Data protection impact analysis or DPIA;
4. Notification of personal data violations to the Supervisory Authority and communication to the data subjects if necessary;
5. Liaising and co-operating with the DPO of the Data Controller customers and the DPO of the Subcontractors to ensure compliance with the GDPR rules.

To reinforce the independence of the DPO and the absence of any conflicts of interest, the OPTORG Group guarantees the following to the DPO:

1. To receive no instructions concerning the performance of his duties;
2. Not to be relieved of his duties or penalised for the performance of its duties;
3. To report directly to the highest level of management.

5.2. DATA CONTROLLER

The Data Controller named in this Personal Data Protection Policy is OPTORG Company, a Limited Company with Management Board and Supervisory Board, with a capital of 38 952 240 euros, registered with the Trade and Companies Register of Nanterre under no. 552 126 385, having its registered office at 49-51, Quai de Dion Bouton - 92800 Puteaux – France, whose legal representative is Mr. Tarafa MAROUANE, Chairman.

The OPTORG Company determines the purposes and means of all processing for which it is the data controller.

5.3. OPERATIONAL DATA CONTROLLERS (ODCs)

ODCs are named within each business unit and operating unit. They are the point of contact for the DPO in their area of responsibility. Their main tasks are as follows:

1. Organising feedback on all new data processing projects to allow exchange with the DPO;
2. Ensuring the implementation and updating of the register of processing activities in their perimeter;
3. Reporting any suspected personal data violations as soon as possible.

6. DATA STORAGE

All OPTORG Group Data Centres in which PD is able to be hosted are located in France or one or more EU countries.

7. OPTORG GROUP'S COMMITMENTS AS DATA CONTROLLER

The OPTORG Group is the Data Controller when it determines the purposes and means of its personal data processing.

7.1. COMPLIANCE WITH GDPR OBLIGATIONS

As the Data Controller, the OPTORG Group must respect the following principles:

1. Appointment of a DPO;
2. Use of personal data for explicit, legitimate and determined purposes in collaboration with the OPTORG Group's business units;
3. Collection and processing of strictly useful PD: The OPTORG Group thus applies the concept of Privacy by Default which protects data subjects from excessive data collection;
4. Conservation of collected PD not exceeding the necessary duration and commensurate with the achievement of the goals. At the end of this period and the deadlines provided by the standards and authorisations of CNIL or by law, PD is deleted on all media and backups;
5. Communication of the PD only to authorised recipients strictly in the context of the previously defined purposes;
6. Selection of Subcontractors according to their technical and organisational guarantees ensuring the protection of the data entrusted to them;
7. No transfer of collected data to third parties other than affiliated companies of the OPTORG Group involved in the performance of the contract;

8. A policy of supervision of personal data transfers outside of the EU in the event of intragroup or other transfers (CCT 2010/87/EU, 2016/2295 and 2016/2297);
9. The previous, clear and transparent notification of the data subjects about the purpose of use of their data, the optional or mandatory nature of their answers on forms, their rights and how they can exercise these rights effectively;
10. The collection of explicit, informed, active and unambiguous consent of the data subjects for the processing of their PD;
11. Conducting impact assessments for processing that may pose a high risk to the rights and freedoms of individuals;
12. The design of tools and systems that, at the core of their functionalities and development, involve respect of the GDPR and the protection of the data of data subjects. The OPTORG Company thus applies the concept of Privacy by Design which allows the development of responsible tools and systems;
13. A security policy ensuring that all measures are taken to prevent personal data violations, informing CNIL and, if applicable, the data subjects within 72 hours, and documentation of remedies made following a violation;
14. Respect for codes of conduct or use of a certification mechanism.

7.2. COMPLIANCE WITH SECURITY OBLIGATIONS FOR PERSONAL DATA PROCESSING

The OPTORG Group has developed an Information Systems Security Policy (ISSP) to ensure the security of infrastructure, resources and application systems.

It has implemented the following security measures to ensure a level of security adapted to the processing risks:

1. Awareness raising and user authentication;
2. Managing authorisations;
3. Tracking access and managing incidents;
4. Securing workstations and mobile computing;
5. Protecting the internal computer network;
6. Securing servers and websites;
7. Backing up and planning for business continuity;
8. Archiving securely;
9. Supervising the maintenance and destruction of data;
10. Managing Subcontractors;
11. Securing exchanges with other organisations;
12. Protecting the premises;
13. Supervising IT developments;
14. Encryption and guaranteeing integrity.

7.3. RESPECT FOR PRIVACY BY DESIGN AND PRIVACY BY DEFAULT REQUIREMENTS

The concepts of Privacy by Design and Privacy by Default allow the implementation of the "data minimisation" principle, ensuring that data collected, both qualitatively and quantitatively, is strictly necessary for processing.

7.3.1. TECHNICAL AND ORGANISATIONAL MEASURES IN PRIVACY BY DESIGN

To meet the GDPR requirements, the OPTORG Group has implemented the following measures concerning PD:

- Minimising PD processing;
- Pseudonymising PD as soon as possible;
- Guaranteeing transparency of the purposes and processing;
- Ability of data subjects to control the processing of their PD;
- Implementation of security systems.

7.3.2. TECHNICAL AND ORGANISATIONAL MEASURES IN PRIVACY BY DEFAULT

The OPTORG Group implements appropriate technical and organisational measures to ensure that only the necessary PD is processed by default.
These measures relate to:

- The amount of PD collected;
- The extent of its processing;
- Its period of storage;
- Its accessibility.

The measures described above guarantee by default that personal data is not made accessible to an indefinite number of persons without the consent of the data subject.

8. COMMITMENTS OF THE OPTORG COMPANY AS A SUBCONTRACTOR

The OPTORG Group acts as a Subcontractor when the Customer has the status of Data Controller for personal data.

With regard to the Subcontracting activities associated with European contracts, in its implementations, in addition to the various legal devices, the OPTORG Group relies on the recommendations of the **Subcontractor's Guide** [1], published by CNIL in September 2017, summarised as follows:

1. Designation of a Data Protection Officer (DPO) who acts as a representative in the EU for contracts concluded directly between a European principal Customer and a Group subsidiary established outside of the European Union;
2. Definition of the responsibilities of the principal Customer and the OPTORG Group concerning the roles of:
    a) Subcontractor;
    b) Data Controller;
3. Detailed contractual management of Subcontracting relationships to take the GDPR rules into account;
4. Prohibition of personal data transfers outside of the European Union or to a country not recognised by the European Commission as having a sufficient level of protection, unless this transfer is based on:
    - Standard Contractual Clauses (CCT 2010/87/EU) adopted by the European Commission regulating the personal data transfer outside of the EU;
    - An appropriateness decision;
5. Respect for the purposes of subcontracted processing activities and traceability of the Customer's instructions;
6. Informing the principal Customer and obtaining its consent if one or more Subsequent Subcontractor(s) is/are used;
7. Providing the Customer with documents to help it meet its regulatory obligations as the Data Controller;

[1] https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

8. Traceability of actions to access or handle PD;
9. Keeping records of processing activities subcontracted by the Customer;
10. Immediate notification of any detected events in violation of personal data protection rules;
11. Assistance in performing data protection impact studies whenever possible and desired by the principal Customer;
12. Regular training and awareness raising of OPTORG Group staff on the principles of confidentiality and obligations related to personal data protection regulations;
13. Permanent ability to demonstrate compliance with obligations including guarantees of:
    a) Privacy by Design;
    b) Privacy by Default;
    c) Creation of organisational and technical security for PD.

To preserve the security and confidentiality of processed personal data, the OPTORG Group undertakes to create:

1. Physical security measures to prevent unauthorised persons from accessing its infrastructure;
2. A permissions management system that limits access to premises and data to authorised persons only in the scope of their duties and activity perimeters;
3. A system of physical and/or logical isolation of its different Customers;
4. A strict password management policy for strong authentication of users and administrators;
5. Ensuring that, during processing, during transfers and after storage, personal data cannot be read, copied, modified or deleted without authorisation;
6. A system allowing the tracking of all actions performed in our information system that, according to the regulations in force, creates reports in event of incidents affecting the Customer's data.

The OPTORG Group may have access to customer data:

1. As part of its legal obligations following judicial and/or administrative requests;
2. To ensure the correct functioning of the services;
3. In the context of support services that may involve remote access to Customer data by other entities in the OPTORG Company located in countries not recognised by the European Commission as having a sufficient level of protection.

In all these cases, access to personal data is subject to:

1. The transfer rules explained above;
2. Accreditations and special authorisations by the Customer.

8.1. CUSTOMER INSTRUCTIONS

The OPTORG Group undertakes to process personal data:

- In the context of the binding contract with its Customer;
- With respect for the documented instructions communicated by the Customer during the performance of the service.

The OPTORG Group must inform the Customer immediately if it considers that any Customer instruction constitutes a violation of the GDPR, this DPP or other provisions of EU or French law regarding personal data protection. This information must be sent in writing and within a timeframe allowing it to be considered by the Customer.

8.2. FATE OF DATA AT THE END OF THE SUBCONTRACTING CONTRACT

As the Data Controller, the OPTORG Group deletes data on a regular basis according to legal requirements.

As a Subcontractor and at the end of the processing service, the OPTORG Group undertakes to:

- Process data only with documented instructions from the Customer;
- Delete or return all data at to Customer's discretion;
- Destroy all existing copies and send the Customer a destruction certificate for all existing copies of its data.

9. DATA SUBJECTS OF PD PROCESSING

The OPTORG Group, as the Data Controller, performs processing of PD communicated directly by the following categories of natural persons:

1. Website and extranet visitors (consultation);
2. Website and extranet users (submission of application forms, etc.);
3. Prospects;
4. Customers;
5. Commercial partners;
6. Suppliers and Subcontractors;
7. Employees and directors of the OPTORG Group or its subsidiaries;
8. Candidates/Temporary workers;
9. Retirees and persons previously employed by the Company;
10. Family, dependents or other persons connected to the OPTORG Group employees through a work contract.

10. PERSONAL DATA PROCESSED

This DPP applies to processing of personal information of candidates and employees of the OPTORG Group, in the context of:

- Recruitment activities conducted both online through its website or through third-party or offline websites, at recruitment events or in phone or face-to-face interviews;
- Human resources management and execution of the employment contract.

The OPTORG Group processes the following categories of personal information according to the conditions in sections 9 and 14 of this DPP:

1. **Identification/marital status data:** Surname, forename, title, postal and/or e-mail address, phone number, social-security number for the pre-employment declaration (DPAE) or nominative social declaration (DSN) with URSSAF;
2. **Professional data:** Training, diplomas, certificates and attestations, foreign language knowledge, competencies, curriculum vitae, professional references, professional evaluations, follow-up of professional training requests and training periods, evaluation of knowledge and training, dates of evaluation interviews, professional skills of the employee, assigned objectives, obtained results, assessment of professional skills based on objective criteria and having a direct and necessary link to the employment held, observations and wishes of the employee, career development forecasts, employee activity tracking documents, expense reports,

annual reports, professional elections, monitoring and maintenance of computer equipment made available, vehicles and payment cards, date and conditions of employment or recruitment, date, purpose and reason for changes made to the employee's professional situation , career simulation, employee's desires in terms of employment, disciplinary penalties excluding those resulting from amnestied acts, administrative follow-up of medical visits, criminal record (B3);

3. **Personal life data:** Marital status and number of children, nationality, immigration and visa status, hobbies, leisure, driving licence category, geographical mobility, availability times;
4. **Economic and financial information:** gross salary, salary requirements, bank details for salary payment, compensation information (variables, bonuses, etc.);
5. **Connection data:** IP address, connections and logs of employee logins, management of IT tools, telephony management (called numbers, incoming numbers, identity of phone service user, etc.), videosurveillance (etc.), geolocation, workplace access control, data regarding payment of meals, checking of schedules (identification items and data used for monitoring working times), access rights to applications and networks.

The OPTORG Group may need to make this PD available to:

- Other Group entities;
- External service providers such as payroll providers, etc.

In compliance with this DPP, the OPTORG Group undertakes to limit PD collection to what is strictly necessary.

11. SPECIFIC CATEGORIES OF PROCESSED PERSONAL DATA

The specific categories of PD are Sensitive Data in the GDPR sense of the term.
This means genetic or biometric data allowing the unique identification of natural persons and unique National Identification Number (NIR for France) such as social-security numbers or data concerning:

- Racial or ethnic origin;
- Political views;
- Religious or philosophical beliefs;
- Trade-union memberships;
- Health;
- Criminal convictions or offences;
- Sexual orientation.

These particular categories of PD cannot be processed without the explicit consent of the data subjects, unless the processing is authorised on other legal grounds.
In any case, the OPTORG Group ensures compliance with the regulations in force.

12. PURPOSES OF APPLICABLE PROCESSING AND LEGAL BASIS

The GDPR requires that any personal data processing has a legal basis.
The OPTORG Group must process all personal data according to the defined purposes and applicable legal bases, as defined by the GDPR and set out below:

1. Consent of the data subject;
2. Compliance with a legal obligation;
3. Execution of a contract or the execution of pre-contractual measures;
4. Safeguarding the vital interests of the data subject or another natural person;
5. Execution of a task of public interest or a task falling within the exercise of the public

authority in which the Data Controller is involved;

6. For the purposes of legitimate interests pursued by the Data Controller, provided that the interests or fundamental rights and freedoms of the data subject are not violated.

The OPTORG Group reserves the right to include specific purposes which must be communicated to the data subjects on specific contractual media supplementing or deviating from this Personal Data Protection Policy.

12.1. CONSENT

According to the GDPR and whenever the OPTORG Group acts as the Data Controller, it must seek to obtain consent from the data subjects for the purposes that require it.

12.1.1. PROCESSING PURPOSES BASED ON CONSENT

The following purposes require explicit consent from the data subjects:

1. Cold calling for products and services;
2. Commercial prospecting by e-mail;
3. Collection of traffic statistics for OPTORG Group websites;
4. Creating files for business statistics purposes;
5. Participation in commercial promotional transactions;
6. Improvement of customer experience;
7. Conducting satisfaction surveys;
8. Geolocation;
9. Cookies.

12.1.2. PROCESSING PURPOSES NOT BASED ON CONSENT

Where based on the execution of one or more contracts or the execution of pre-contractual measures, to comply with the regulations in force or to allow the OPTORG Group to protect its legitimate interests, the following purposes do not require explicit consent from the data subjects:

1. Risk analysis and determination of customer or prospect needs;
2. Exercise of advisory duties;
3. Execution of employment contracts;
4. Improvement of customer experience;
5. Conducting satisfaction surveys;
6. Participation in commercial promotional transactions;
7. Execution of all public policy obligations;
8. Creating files for statistical purposes.

12.1.3. COLLECTION AND TRACEABILITY OF CONSENT

As the Data Controller, the OPTORG Group must demonstrate that data subjects' consent to the processing of their PD was obtained in a free, informed and unambiguous manner. The traceability mechanism used by the OPTORG Group allows it to meet this major requirement of the GDPR by:

- Providing proof of consent;
- Ensuring the integrity of this consent over time.

SPECIAL CASE OF PROFILING

The OPTORG Group may use and compile PD for profiling purposes. Automated processing is used to assess, analyse and predict the preferences or interests of data subjects but may have legal consequences that significantly affect the data subject.

The OPTORG Group undertakes to inform the data subjects and obtain their explicit consent before any profiling-related processing.

13. USE OF COOKIES

Visitors to and users of the OPTORG Group's websites should refer to the legal notices on these sites for conditions of use of cookies.

14. OPTORG'S COMPLIANCE WITH THE PRINCIPLE OF ACCOUNTABILITY

The OPTORG Group has implemented internal mechanisms and procedures to show its continuous compliance with the rules imposed by the GDPR, in particular by implementing technical and organisational measures and a documentation obligation. These measures are reviewed and updated when necessary.

The OPTORG Group can thus demonstrate its compliance with the principles of personal data processing such as:

1. Lawfulness, loyalty and transparency of processing;
2. Purpose limitation;
3. Minimisation;
4. Accuracy of PD;
5. Limitation of storage periods;
6. Integrity and confidentiality of PD.

14.1. IMPLEMENTATION OF TECHNICAL MEASURES

1. Encryption of confidential data;
2. Management of access rights;
3. Anti-network intrusion tools (firewall, antivirus);
4. Password policy (complexity, regular changes);
5. Protection via secure streams (TSL/SSL, https, sftp).

14.2. IMPLEMENTATION OF ORGANISATIONAL MEASURES

1. Data mapping procedure;
2. Contract review (Subcontractors, partners, employees, customers);
3. Awareness raising/training of business unit and IT teams;
4. Keeping of the register of processing activities;
5. Data minimisation policy (Privacy by Design/Privacy by Default);
6. Risk analysis (PIA);
7. Management of persons' rights.

14.3. DOCUMENTATION OF ACCOUNTABILITY

Being aware of the importance of protecting PD, the OPTORG Group has created all necessary documentation to demonstrate its GDPR compliance.

This documentation is regularly updated and includes:

1. **Internal procedures regarding Privacy by Design, Privacy by Default and data protection impact assessments, including:**
    a) Documentation demonstrating the consideration of PD protection in the implementation of new products;
    b) Impact analysis models and impact assessments performed, including their updates;
    c) Reasons leading the Data Controller not to perform an impact analysis for potentially high-risk processing;
    d) Rules for reviewing the impact assessments to be performed in the event of changes in processing or after a certain time (every 3 years).

2. **Appointment of a DPO**
    a) Tasks letter of the DPO;
    b) Reasons for not appointing a DPO if applicable;
    c) Statement by the DPO to CNIL;
    d) Evidence that the DPO reports regularly to the highest level of management;
    e) Professional qualifications of the DPO.

3. **Contractual relations with Subcontractors**
    a) Contracts with Subcontractors;
    b) Follow-up policy governing Subcontracting relationships (questionnaire templates sent regularly to Subcontractors and replies to these questionnaires);
    c) Audit procedures for Subcontractors;
    d) Results of audits performed and actions taken as a result;
    e) Co-responsibility agreements with other Data Controllers involved in PD processing.

4. **Security policy**
    a) Information systems security policy and documentation describing the measures taken to ensure PD security (pseudonymisation and encryption);
    b) Means to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services;
    c) Means to restore the availability of and access to PD within the appropriate time in the event of a physical or technical incident;
    d) Test plans to test, analyse and regularly evaluate the effectiveness of technical and organisational measures to ensure processing security and results of security tests performed;
    e) The management policy for authorisations and access.

5. **Violations of personal data**
    a) The internal policy regarding personal data violations and the details of contact persons;
    b) The register of personal data violations and notifications to data subjects and CNIL;
    c) Items justifying the Data Controller's decision not to send notifications to data subjects in the event of violations of their PD.
6. **Transfers of personal data to third countries and transfer mechanisms implemented:**
    a) Summary of PD transfers and the transfer mechanism used for each;
    b) Documentation of the implementation of transfers according to the selected mechanism:

i. BCRs and their approval decision by CNIL;
ii. The standard contractual clauses for personal data protection signed with PD importers and exporters;
iii. The ad-hoc contractual clauses approved by CNIL and the approval decision;
iv. Documents regarding transfers made based on the "exceptions" in Article 49 GDPR, such as proof of consent of data subjects or analysis of balancing of interests of data subjects and Data Controllers;
v. Appropriateness decisions.

7. **Personal data protection policy**
   a) Personal data confidentiality policy (DPP);
   b) PD storage policy (storage time, destruction times and intermediate archiving rules);
   c) Procedures implemented to ensure respect for the rights of data subjects;
   d) Templates of the main information and consent clauses in contracts, on the website and other main communication channels with data subjects;
   e) Documentation regarding the management of requests from data subjects, including requests for the exercise of their rights and the answers given;
   f) The mechanism implemented to ensure the traceability and monitoring of the rights exercised by data subjects.

8. **Codes of conduct and certification:**
   a) Document attesting to respect for a code of conduct and related documentation;
   b) Certifications.

9. **Compliance control plan**

10. **Correspondence with CNIL**
    a) History of correspondence with CNIL
       i. Prior consultation following an impact analysis;
       ii. Notification of personal data violations;
       iii. Checking or requesting information by CNIL.

11. **Keeping the Processing Register**

All processing must be added to the Processing Register.
To this end and according to its roles, the OPTORG Group keeps several registers:

1. Processing Register as the Data Controller, in which processing based on consent of data subjects is separated from processing based on legal grounds;
2. Processing Register as a Subcontractor;
3. Processing Register for notification of PD violations.

Record keeping is dynamic, with updates based on the progression of existing processing (including removal) and implementation of new processing.

15. STORAGE TIME OF PD

The PD of the data subjects is kept for the purposes stated, in compliance with the legal requirements in force, particularly in civil, fiscal, commercial and criminal matters.

Unless otherwise requested, data for the purpose of managing the recruitment is stored for two years from its receipt or the last contact with the candidate.

Data used to manage staff is stored for the duration of the employee's contract. Some data may be stored beyond this, but still within the statutory time limits set by the regulations.

Data for the purpose of prospecting or commercial canvassing is stored for three years from receipt or the last contact with the prospective customer.

Intermediate archiving: Access to PD stored in this context is strictly limited. At the end of the storage period, the PD must be destroyed or anonymised so that it is no longer possible to identify the data subjects.

16. PERSONAL DATA TRANSFER

The OPTORG Group undertakes to comply with all obligations regarding personal data transfer to third countries and, in particular, will conclude a binding legal contract with recipients of the data such as Standard Contractual Clauses or BCRs.

The OPTORG Group undertakes not to transmit data to its subsidiaries or "Data Recipient" third parties unless strictly necessary.

In this case, the OPTORG Group must ensure that "Data Recipients" have at least the same level of security in their data processing.

According to the GDPR, the Subcontracting of data must be subject to a written agreement between the OPTORG Group and the Subcontractor, with the latter committing not to perform any data transfer without the authorisation of the OPTORG Group.

If data transfers are to be made outside of the European Union, the OPTORG Group undertakes to proceed only under these conditions:

- The "Data Recipient" is in a state considered by the European Commission to provide an adequate level of protection;
- The "Data Recipient" has Standard Contractual Clauses of the European Commission;
- Any Subsequent Subcontractor located outside of the EU must meet at least one of the conditions set out above.

17. RIGHTS OF PERSONS

According to the regulations, data subjects have the:

1. Right of information before any PD collection;
2. Right to confirmation that PD is or is not being processed;
3. Right of access to obtain the following information:
    a) Purposes of processing;
    b) Categories of personal data concerned;
    c) Recipients or categories of recipients to whom personal data has been or will be communicated;
    d) Appropriate safeguards in the event of transfer of data to a third country;

e) Expected data storage period or criteria used to determine this period;
f) Existence of the right to ask the Data Controller to rectify or delete data or limit its processing, or the right to oppose it;
g) Right to lodge a complaint with CNIL;
h) Source information in the case of indirect collection of PD;
i) Existence of automated decision-making and/or profiling and consequences for data subjects;

4. Right to rectification;
5. Right to limitation;
6. Right to be forgotten;
7. Right of objection to specific processing for which explicit consent was required (withdrawal of consent);
8. Right to data portability;
9. Right not to be subject to a decision based on an automated process;
10. Right not to be subject to profiling;
11. Post-mortem right.

Any person concerned may exercise his rights, accompanied by proof of identity either:

- By sending an e-mail to dpo@optorg.com ;
- By mail to:

OPTORG Company
Data Protection Officer
49-51, Quai de Dion Bouton 92800 Puteaux – France

The OPTORG Group:

- Reserves the right to request additional documents from the applicants justifying their identity;
- Informs data subjects that, according to the rules of public order in force, certain data or certain purposes cannot be subject to a favourable response to requests.

If data subjects consider that they were not able to exercise their GDPR rights or any legal provisions in force concerning data protection, they may lodge a complaint to:
Commission nationale de l'informatique et des libertés (CNIL) (National Commission for Information Technology and Liberties)
3 place de Fontenoy – TSA 80715 – 75334 Paris Cedex 07.

18. ENHANCED CONFIDENTIALITY AND ACCESS TO PD

All employees and agents of the OPTORG Group are made aware of the principles of data protection through regular training tailored to their activities and responsibilities. They only have access to the information necessary for their activities.
Access to sensitive data is subject to authorisations and controls.
The OPTORG Group further guarantees that its employees are subject to a strict confidentiality obligation and undertakes to have an individual confidentiality agreement signed by all persons able to access personal data.
The OPTORG Group also undertakes to ensure that its Subcontractors and any Subsequent Subcontractors are bound by this specific obligation.
However, despite all the rigour and precautions taken to implement PD protection, it is not possible to guarantee its absolute security due to the evolution of intrusion techniques and unavoidable risks that may occur during transmission.

19. VIOLATION OF PERSONAL DATA

For the purposes of the GDPR, a PD violation is a security violation resulting in accidental or unlawful destruction, loss, alteration, disclosure or unauthorised release of PD transmitted, stored or otherwise processed, or unauthorised access to such data.

19.1. NOTIFICATION OF PD VIOLATIONS AS A SUBCONTRACTOR

It is the Customer's sole responsibility to notify CNIL of any security violations.
The OPTORG Group undertakes to notify the Customer as soon as possible and allow the latter to comply within the legal deadline of maximum 72 hours with any personal data violation that it has suffered.

In case of delay in communication of the violation, the OPTORG Group must include with its notification the reasons for this delay.

The data violation must be communicated to the contact person designated by the Customer and must specify:

1. The nature of the data violation, including if possible:
    a) Categories and approximate number of persons affected by the violation;
    b) Categories and approximate number of personal data records affected;
2. Name and contact details of the OPTORG Group's DPO;
3. Likely consequences of the data violation;
4. Measures already taken or proposed to remedy them.

If the OPTORG Group is unable to provide all this information within the deadline, it must proceed in two stages by sending:

1. Immediate initial notification upon finding the violation;
2. A further notification within 72 hours of the initial notification if possible.

In the event of data violation, the OPTORG Group must, as soon as possible, take all necessary measures to remedy and reduce the impact of the violation and must inform the Customer of the measures taken and the expected and observed results.

The OPTORG Group is committed to collaborating actively with the Customer to be able to meet:

- Its regulatory and contractual obligations;
- The requests of CNIL.

19.2. NOTIFICATION OF PD VIOLATIONS AS THE DATA CONTROLLER

As the Data Controller, the OPTORG Group strives to ensure the security of the PD processing performed to prevent any violation of them.

Nevertheless, in the event of personal data violations, the OPTORG Group must respect the obligation to notify CNIL of the violation in question as soon as possible, and if possible within 72 hours of becoming aware of it, unless the violation in question is not likely to pose a risk to the rights and freedoms of the data subjects.

Beyond 72 hours, the notification that the OPTORG Group will communicate to CNIL must

indicate the reasons for the delay.

19.3. PROCESS FOR MANAGING AND PREVENTING RISKS AND INCIDENTS

To prevent violations and limit their impact, the OPTORG Group has defined and implemented an intrusion detection system and an incident management procedure.

19.3.1. DETERMINATION OF PREVENTATIVE MEASURES

1. Setting up an effective and secure backup solution;
2. Using encryption methods;
3. Limiting access to personal data;
4. Traceability of accounts with "global access" to a database;
5. Secure storage of passwords;
6. Permanent monitoring of potential vulnerabilities in the technologies used and updating of software;
7. Informing employees of the consequences of potential data violations;
8. The application of Privacy by Design and Privacy by Default;
9. The arrangements made in the context of data protection impact analyses.

19.3.2. POSSIBLE NOTIFICATION TO DATA SUBJECTS

When a PD violation is likely to pose a high risk to the rights and freedoms of the data subject, the OPTORG Group as the Data Controller undertakes to:

- Keep the data subject informed as promptly as possible;
- Offer recommendations and protective measures to reduce the harm suffered.

The notification

- Must be clearly and simply worded so as to be easily understandable;
- Must contain the same information communicated to CNIL.

20. CHECKING BY CNIL

The OPTORG Group is required to co-operate with CNIL at the request of the latter.
In the event that the checking relates to processing in the name and on behalf of one of its Customers, the OPTORG Group undertakes to inform it immediately and make no commitment to it.

In the event of a CNIL check with a Customer concerning the services delivered by the OPTORG Group as a Subcontractor, the latter undertakes to co-operate with the Customer and provide it with any information that CNIL may need.

In the event that the checks performed relate only to the processing performed by the OPTORG Group as the Data Controller, OPTORG is prohibited from communicating or reporting the personal data of Customers for which it is the Subcontractor.

21. AUDITING

To ensure compliance with the GDPR obligations, Customers can perform audits once a year in the form of a questionnaire or request for information on the level of GDPR compliance of the OPTORG Group.

Moreover, in the same spirit, the OPTORG Group as the Data Controller will exercise its audit right on its own Subcontractors and will proceed in the same way with Subsequent Subcontractors if necessary.

22. REVISION

This DPP will be revised as necessary in the following cases:

- Changes to jurisprudence;
- Decisions by CNIL;
- New regulations concerning personal data protection.