CENTRE DE CHIRURGIE PLASTIQUE ET ESTHÉTIQUE DR. ASSASSI

(the *"**Company**"*)

DATA PROTECTION POLICY

REGISTERED OFFICE AT: 71 Rue des Glacis L-1628 Luxembourg (RCSL n. (*)).

1. INTRODUCTION

The Company holds personal data (the "**Personal Data**") of the following natural persons:

1. Internal Data Subjects:
    - Shareholders;
    - Employees;
    - Investors;
    - Connected counterparties of the same group.
2. Suppliers:
    - Service providers;
    - Consultants.
3. Customers (Patients).

(hereinafter all referred to as "**DATA SUBJECTS**").

The data protection policy (the "**Policy**") sets out how the Company seek to protect Personal Data and ensures that the staff of the Company understands the rules governing the use of Personal Data to which specified people are entitled to have access in the course of their work.
Personal Data must be collected and dealt with appropriately, whether on paper, a computer, or recorded on other material.
There must be safeguards in place to ensure this under the Policy.

In order to comply with the Policy, the Company shall ensure that it has at least one legitimate reason to collect, use, manage or disclose Personal Data. In some circumstances the consent of the DATA SUBJECTS may not be necessary.

In particular, the Policy requires that the Company ensures that the board of the Company ("**Board**") is consulted before any new significant data processing activity is initiated to ensure that relevant compliance steps are addressed.

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (the "**GDPR**") addresses the rapidly changing technology environment which has created a variety of new options concerning the collection, storage, sharing and use of Personal Data.
The GDPR is intended to unify the approaches of EU member states to data regulation and to ensure all data protection laws are applied identically in every country within the EU. It also introduces new expectations with regard to consent to use DATA SUBJECTS' data and the need to be very clear on how data are used.
The Policy should be read in conjunction with:

- the Data Protection Checklist;
- the Data Protection Impact Assessment.

2. DEFINITIONS

Data subject	The individuals in relation to whom the Company is holding personal information. In this frame, they are: 1. Internal Data Subjects: ○ Shareholders; ○ Employees; ○ Investors; ○ Connected counterparties of the same group. 2. Suppliers: ○ Service providers; ○ Consultants. 3. Customers (Patients).
DPA	In Luxembourg the DPA (Data Protection Authority) is the Commission Nationale de Protection des Données, 1, avenue du Rock'n'Roll, L-4361 Esch-sur-Alzette, Tél. : (+352) 26 10 60 -1, www.cnpd.lu.
Personal data	The information in hard and electronic copy relating to DATA SUBJECTS held by the Company, transferred to or exchanged with third parties, or held by third parties on behalf of the Company. The Company collects the following Personal Data: contact details, residential address, email address, educational background, financial and pay details, details of certificates and Diploma, education and skills, marital status, nationality, job title, CV, proof of origin of funds, tax numbers/TIN, IBAN/Bank details, investment data.
Record of Data Processing Activities	The register where the Company or any organization acting on behalf of it shall, according to Article 30 of GDPR, maintain a record of processing activities under its responsibility.
Relevant Persons	Personal Data will be processed or viewed by: • Shareholders; • Members of the Board; • Key people of the Company.
Sensitive personal data	Personal Data about DATA SUBJECTS' racial or ethnic origin, political opinions, religious or similar beliefs, physical or mental health or condition, criminal offences, or related proceedings. In compliance with the GDPR, the processing of sensitive Personal Data is strictly controlled in accordance with the Policy.

3. SCOPE

The Policy applies to all Personal Data as defined in section 2 ("*Definitions*").

All departments which will need Personal Data to meet the contractual and legal obligations of the Company will have access to such information and therefore all staff of the Company will receive specific training to understand the importance of the confidentiality of Personal Data and to sign a confidentiality clause.

The Company staff must be familiar with the Policy and comply with its terms.

The Policy supplements other policies relating to the use of internet and email use.

The Company may supplement or amend the Policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

4. OUR PROCEDURES

Fair and lawful processing

Personal Data must be processed fairly and lawfully in accordance with GDPR. Accordingly, the Company shall not process Personal Data unless the DATA SUBJECT concerned has given his or her consent.

Processing and use of Personal Data
Personal Data must be processed in order to fulfil the business purpose of the Company and meet its legal obligations. Personal Data will only be processed lawfully and fairly in order to fulfil the Company's purpose and meet its legal obligations.
The Relevant Persons or those acting on behalf of the Company shall comply with the GDPR.

Justification for Personal Data
The Company will process Personal Data in compliance with data protection principles:

1. Personal Data shall be processed fairly, lawfully and in a transparent manner.

2. Personal Data shall be gathered for specified, legitimate and explicit purposes; additionally they shall not be further processed in any manner incompatible with those purposes.

3. Personal Data shall be adequate, relevant and restricted to what is necessary to the purposes.

4. Personal Data shall be accurate and, where necessary, kept updated.

5. Personal Data shall be kept in a form permitting the identification of DATA SUBJECTS for no longer than is necessary for the business purposes.

6. Personal Data must be processed in a way ensuring proper security of them, including the use of appropriate technical and organisational measures to protect Personal Data against accidental damage, destruction or loss.

7. Personal Data shall be processed in accordance with the rights of DATA SUBJECTS under the Policy.

8. Personal Data shall not be transferred to a country or organisation outside the European Economic Area unless that country or organisation is considered by the European Commission to be able to ensure an adequate level of protection for the rights and freedoms of DATA SUBJECTS in relation to the processing of Personal Data.

The Company documents any additional justification for the processing of sensitive data.

5. ACCURACY AND RELEVANCE

The Company will ensure that processed Personal Data are accurate, adequate, relevant and not excessive, given the purpose for which they were obtained.

The Company will not process any Personal Data obtained for unrelated purposes unless the concerned DATA SUBJECT gives his or her consent to do so or reasonably expects such process.

DATA SUBJECTS may ask the Company to correct inaccurate Personal Data relating to them. If the Company believes that Personal Data about DATA SUBJECTS is inaccurate the Company is required to inform the Relevant Persons, involved in the processing of Personal Data.

6. CONSENT AND CONDITIONS FOR PROCESSING DATA

Pursuant to Article 6 (1) of the GDPR, the processing of Personal Data is lawful if at least one of the following points applies:

6(1)(a)	The DATA SUBJECT has given his or her consent;
6(1)(b)	Processing is necessary for the performance of a contract with the DATA SUBCJETC subject or to take steps to enter into a contract;
6(1)(c)	Processing is necessary for compliance with a legal obligation to which the company is subject;
6(1)(d)	Processing is necessary to protect the vital interests of a DATA SUBJECT or another person;
6(1)(e)	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority;
6(1)(f)	Processing is necessary for the purposes of legitimate interests.

7. PRIVACY NOTICE - TRANSPARENCY OF DATA PROTECTION

It is of significant importance that the Company is transparent in providing accessible information to DATA SUBJECTS about how it will use Personal Data.

The notice:

- Sets out the purposes for which the Company holds Personal Data;
- Highlights that the Company may require us to give information concerning DATA SUBJECT to third parties;
- Provides that Company stakeholders have a right of access to the Personal Data.

8. PERSONAL DATA

DATA SUBJECTS must ensure that Personal Data held by the Company are accurate and updated as required.
For instance, if personal circumstances change, the DATA SUBJECT is required to inform the Company in order to update his or her records.

9. SHARING PERSONAL DATA

It is responsibility of the Company to ensure that the sharing of Personal Data to third parties takes place in a secure manner and in compliance with the GDPR.

1. Internal Data Subjects:
    - Connected counterparties of the same group.
2. Suppliers:
    - HR providers;
    - Payroll providers;
    - External accountants.
3. Institutional counterparties:
    - Local Authorities;
    - Banks;
    - Pension providers.

The Company does not send direct marketing material to anyone unless it has an existing business relationship with them in relation to the services being marketed.

10. SENSITIVE PERSONAL DATA

The Company processes, *inter alia*, Sensitive Personal Data, as defined in section 2 ("*Definitions*"), which are mainly collected through a document called Patient Questionnaire filled up and executed by the concerned DATA SUBJECT (mainly the Patient), made of two sections: section one consists of a two pages information sheet regarding Personal Data and

Sensitive Personal Data; section two consists of a five pages consent letter which gives DATA SUBJECTS an overview of the GDPR and of the Policy.

The DATA SUBJECT is required to explicit his or her consent to the processing of the data collected in it, unless exceptional circumstances apply or the Company is obliged to do so by law (e.g. to comply with legal obligations to ensure health and safety at work or to its Patients).

Each consent to process Sensitive Personal Data needs to clearly include what the relevant data are, why they are being processed and to whom they will be disclosed.

Sensitive Personal Data will be processed on the following grounds:
- Explicit consent has been given;
- Processing is necessary for the purposes of carrying out the obligations;
- Processing is necessary for the reasons of substantial public interest, on the basis of the EU or national Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide specific measures to safeguard the fundamental rights and the interests of the DATA SUBJECT.

The Company processes also a special kind of data - photos - which, when associated to names or codes capable of identifying the DATA SUBJECT, are to be treated as Personal Data or Sensitive Personal Data, as the case may be.

The Company uses higher care while treating this special category of Personal Data, especially in compliance with the following articles of the GDPR:
- Articles 13 and 14. Right of the DATA SUBJECT to be informed in a clear manner about the context of how his or her photos are being used. For example photos cannot be used for reasons other than the one for which consent was had been given;
- Article 15. Right of the DATA SUBJECT to access his or her personal data (photos in this case) on simple request and receive confirmation regarding how these are being used;
- Article 17. Right to erasure, whereas without prejudice to the right of the DATA SUBJECT to apply to the DPA, Individuals have the right to simply request their photos to be returned, deleted or removed for any kind of support that was not originally authorised (i.e. websites, social media or future versions of printed materials).

11.IMPACT ANALYSIS EXERCISES

Data security
The Company keeps Personal Data secure against loss or misuse. Employees have signed a specific confidentiality clause before processing Personal Data on behalf of the Company.

Privacy by design and by default
Privacy by design is an approach to projects that promotes privacy and data protection compliance from the beginning.

The Board/the Relevant Persons will be responsible for ensuring that all data security processes and IT projects commence with a privacy plan.
When relevant, and if it does not have a negative impact on the DATA SUBJECT, privacy settings will be set to the most private by default.

Storing data securely

- When Personal Data are stored in hard copy, they are to be kept in a secure place where unauthorised personnel cannot have access. Personal Data in hard copy will be stored in a separate locked office cabinet and filed as soon as received, after the scan process.
- Personal Data in electronic format are to be kept in a separate environment on the server, provided with a key access code only known to Relevant Persons and IT service providers.
- Printed data are shredded when they are no longer needed – use data deletion processes as set out in the Policy.
- Use of secure remote access software for accessing Company systems from another location.
- The Company encourages all staff to use a password manager to create and store their passwords.
- Devices such as laptops should be locked away when not in use.
- Ensure antivirus and malware software are up to date as well as operating systems on laptops and desktops.
- Mobile phones are password protected and able to have their content accessed/deleted remotely.
- Emails containing Personal Data should not be sent from staff/governor/trustee personal accounts.
- Staff should be vigilant of emails with suspicious attachments, from emails addresses which have similar name configurations hyperlinks and proceed cautiously.
- Ensure staff complete basic “cyber security” training in relation to opening emails, handling Personal Data etc.
- Ensure wireless network is password protected and encrypted.
- Data stored on CDs or memory sticks is encrypted and locked away securely when not being used.
- The Relevant Persons must approve any cloud used to store data.
- Servers containing Personal Data are kept in a secure location or in the cloud, away from general office space.
- Data are regularly backed up in line with the company’s backup procedures.
- All servers containing Sensitive Personal Data are to be approved and protected by security software and a strong firewall.
- Each member of the staff must immediately report any loss or damage of devices in use, e.g. laptops, personal computers to the Relevant Persons.
- Keep a record of third party access to data – e.g. payroll companies, pension providers etc.

12.DATA RETENTION PERIODS

The Company retains Personal Data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the Personal Data were obtained, but if relevant, the length of retention will be determined in a manner consistent with published legal and regulatory data retention guidelines.
Personal Data and documents kept for business extent are treated segregated as described in the Policy and destroyed if requested by the concerned DATA SUBJECT or no longer useful for business purpose or if they are no longer detained in compliance with the relevant laws.

13.DATA DELETION

Pursuant to the GDPR, the Personal Data processed shall not be kept for longer than is necessary for the business purposes of the Company.

Safe destruction of records
Disposal of records which have reached the end of the minimum retention period will be deleted or archived in line with the following guidance and whatever decisions are made, they need to be documented as part of the records management policy within the organization in the Record of Data Processing Activities.

All records containing the following Personal or Sensitive Personal Data shall be destroyed:

- Paper records should be shredded using a cross-cutting shredder.
- CDs / DVDs / Floppy Disks should be cut into pieces.
- Audio / Photos / Video Tapes should be dismantled and shredded.
- Hard Disks should be dismantled and sanded.

Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in the regular waste or a skip unless there is no other alternative.

There are companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way.

Where records are destroyed internally, the process must ensure that all the records are provided with appropriate authorisation of the persons in charge before being destroyed. The destruction must be recorded.
Records should be shredded as soon as the record has been documented as being destroyed.
The destruction/shredding needs to be planned with specific dates and all records should be identified as to the date of destruction.

Staff working for the external provider should have been trained in the handling of confidential documents.

Transfer of information to other media
Where lengthy retention periods have been allocated to records, members of staff may convert hard copy records into media records such as microform or digital media. The lifespan of the media and the ability to migrate data shall always be accurately considered.

Recording of all archiving, permanent destruction and digitisation of records
Sample appendices are provided for the recording of all records to be used. These records could be kept in an Excel spreadsheet or other database format.

14.TRANSFERRING DATA INTERNATIONALLY

There are specific restrictions on international transfers of Personal Data.

No Personal Data must be transferred outside of the European Economic Area (EEA) without first discussing it with the Relevant Persons.

Specific consent shall be obtained from DATA SUBJECTS before transferring their Personal Data outside the EEA.

DATA SUBJECTS must have received appropriate safeguards by the Company (e.g. legally binding instruments between public authorities, binding corporate rules and standard data protection clauses adopted by the European Commission or by the relevant supervisory authority, etc.).

Any transfer of Personal Data anywhere outside the Grand-Duchy of Luxembourg must be approved by the Relevant Persons.

15. SUBJECT ACCESS REQUESTS

The DATA SUBJECTS are entitled, subject to certain exceptions, to request access to information held about them.

No charges should be made to the DATA SUBJECT concerned.

Upon request, the DATA SUBJECT shall have the right to receive a copy of their Personal Data in a structured format. These requests should be processed within one month, provided that there is no undue burden and it does not compromise the privacy of other DATA SUBJECTS.

In order to apply for an access to information, the DATA SUBJECT shall refer such request to the Relevant Persons.
There are also restrictions on the information to which DATA SUBJECTS are entitled to access under the applicable law.

16. RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN)

DATA SUBJECTS are entitled to request that any Personal Data held about themselves is deleted or removed without undue delay if, for instance, the Personal Data are no longer necessary in reference to the business purposes or they have been unlawfully processed.

Any third parties processing such data must also comply with such request.

An erasure request can only be refused if an exemption applies.

17.TRAINING

All the members of the staff of the Company will receive the Policy.

All the Relevant Persons will receive training that will cover:

- The GDPR and
- The Company's Policy, related procedures and best practices.

Training is also provided to the members of the staff of the Company through in-house sessions on a regular basis or whenever there is a substantial change in the law or in the Company's Policy and procedure.

New joiners will receive training on the Company's Policy as part of the induction process.

Additionally, the Company will also organise refresher sessions in order to keep updated the whole staff of the Company in reference to the data protection procedures and best practices.

The Completion of training is compulsory.

18. DATA BREACHES

Each DATA SUBJECT and each member of the staff of the Company shall immediately notify the Relevant Persons if they are concerned about a possible data breach.
Even if a breach is discovered after the relevant time by DATA SUBJECTS or staff members, the Relevant Persons shall be immediately notified.

Reporting breaches
Data breaches must be reported to the DPA without undue delay and, when feasible, within 72 hours after becoming aware of it.

The Company shall document Personal Data breaches, including information about what and how occurred, the effect of the breach and any remedial action taken.
All members of the staff are required to report actual or potential data protection compliance failures.

The DATA SUBJECTS shall be informed of the breach without undue delay in case they are likely to be adversely affected by it.

Checklist for data breaches

1. Inform the DPA within 72 hours;
2. Inform the Relevant Persons to keep records of response to the data breach;
3. Identify key internal and external messaging for communications strategy and issue;
4. Secure IT systems;
5. Stop additional data loss;
6. Inform DATA SUBJECTS: If there is a high risk to the rights and freedoms of DATA SUBJECTS, DATA SUBJECTS must be notified;
7. Identify key issues and extent of data breach;
8. Review protocols about disseminating information about the breach for everyone involved;
9. Begin an in-depth investigation, by using forensics if necessary;
10. Report to police, if considered appropriate;
11. Notify regulators.

What information must a breach notification contain?

1. The nature of the Personal Data breach including, the categories and approximate number of DATA SUBJECTS concerned and the categories and approximate number of Personal Data records concerned;
2. The name and contact details of the Relevant Persons;
3. A description of the likely consequences of the Personal Data breach; and
4. A description of the measures taken, or proposed to be taken, in order to deal with the Personal Data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

19.CONSEQUENCES OF FAILING TO COMPLY

The Company takes compliance with the Policy very seriously.

Failure to comply puts both the staff and the Company at serious risk.
The importance of the Policy means that failure to comply with any legal requirement may lead to disciplinary actions under the Company's procedures which may also result in dismissal.

20. MONITORING

Everyone must observe the Policy.

The Relevant Persons have overall responsibility for the Policy.
They will monitor it regularly to make sure it is being adhered to.

Among the Relevant Persons, the individual below has been appointed as the person of contact for the Data Protection:

CENTRE DE CHIRURGIE PLASTIQUE ET ESTHÉTIQUE DR. ASSASSI

Mr. /Ms. [*]

71 Rue des Glacis
L-1628 Luxembourg

Email : info@dr-assassi.lu

Telephone: (+352) 26 27 02 93