Privacy Policy

GDPR Documentation Series

Prepared by: PhoenixPro
1 December 2020
v.02

Table of Contents

A. Overview

On the 25th of May 2018, the new European data privacy law, known as the General Data Protection Regulation ("GDPR"), has come into force. GDPR defines a specific framework and set of rules for the protection of individuals within the European Economic Area (EEA) with regard to the processing of their personal data.

Any physical or legal person, be it an individual, a company or an organization that collects, stores, manipulates or otherwise processes personal data (hereafter collectively referred to as "processing") is affected, and is required to adopt appropriate technical and organizational measures that make such processing compliant to the provisions of the GDPR. GDPR affects therefore any physical or legal person or body who performs processing irrespective if they are established within or outside the European Union, so long as such physical or legal persons perform processing of personal data for individuals who are in the European Union.

This Privacy Policy has been prepared by Eye Centre Laservision Ltd (hereafter referred to as "Laservision"), with the objective of assisting our patients, employees, vendors, partners and all other interested parties that may be affected, gain an understanding of the measures we have adopted and operate, as part of our own GDPR compliance program and practices. When we mention "Laservision" "we", "us" or "our" in this Privacy Policy, we are referring to legal entity responsible for processing your data, in this case Laservision.

B. Laservision as a Data Controller or Data Processor

In running our business, Laservision is a Data Controller, with access to, and processing of personal data of, our patients, employees and / or suppliers. Laservision is committed to performing such processing in transparent and fair ways, based on processes which are private by design and using appropriate technical and organizational measures in support of security and privacy objectives. This commitment is applicable throughout the lifecycle of personal data processing, including during collection, transmission, use and storage.

Laservision also commits to taking all reasonable steps to ensure that personal data processing is based on a valid legal basis [1]. In certain cases, the processing we perform is dictated by legislation or may be based on our legitimate interests, especially those which emanate from our professional obligations and responsibilities and / or other regulatory frameworks subject to which we perform our work.

C. What is the Basis on Which we Justify Processing of Your Personal Data

In accordance with Article 6 of the GDPR, personal data processing is lawful if at least one of the processing bases described below applies.

- the consent of the data subject (i.e. the physical living person) whose personal data is processed
- processing is necessary in order to enter into a contract to which the data subject is a contractual party or to take action at the request of the data subject before or after a contract is entered into force
- processing is necessary to comply with a statutory obligation of the Data Controller

[1] See definitions in the Glossary to this Privacy Policy

- processing is necessary for the purposes of the legitimate interests pursued by the Data Controller, unless such interest overrides the interest or fundamental rights and freedoms of the data subject who require the protection of personal data, in particular if the subject of the data is a child

- processing is necessary to safeguard the vital interest of the data subject or other natural person

- processing is necessary for the performance of an obligation performed in the public interest or in the exercise of public authority assigned to the Company.

Based on the above, Laservision seeks to ensure that each type of personal data processing we perform is supported by one or more of the above legal bases. With very few exceptions, the legal bases applicable to our operational routines and the resulting personal data processing we conduct are those described in the first four bullets.

D. How Do we Collect Personal Data

In the great majority of cases, we receive the personal data directly from the affected individual (i.e. the data subject"). Typically, such personal data is requested of you when we initiate our relationship (i.e. during the initial Patient Registration process), or in some cases at a later stage, after we commence interacting with each other. There are various means we may accept for receiving personal data including paper-based forms, via email communications or physical exchange of contact information (such as a business card). We may also collect personal data via automated means when data subjects interact with resources we provide (CCTV systems, email submission tools, website logs, etc.).

We may also enhance the personal information we process about data subjects, as a result of the interactions and / or transactions between the data subjects and Laservision.

Finally, in a limited number of cases, we get personal information for the data subjects from 3rd party sources, for example, in the case of patients, medical records from referring Doctors, clinics, hospitals or other medical practitioners. Key examples for other, non-patient scenarios include references from previous employers during an employment application process and other lawful services of similar nature. If the data subject is a representative of one of our suppliers, we may receive their personal information directly from their employer / principal, or from other colleagues of the data subject.

E. Why we Process your Personal Data

We describe below the key ways we use personal information, and the legal bases of processing on which we rely for such processing. We have also identified what our legitimate interests are where appropriate. Generally, the personal data we collect, store and process are used to allow us to meet your medical needs in the most appropriate basis. More specifically, we also use your information to:

- help Laservision understand your medical condition(s), deliver medical services to you and enable us to administrate the necessary medical treatment appropriate to your medical needs and circumstances

- provide you service such as responding to your queries, scheduling appointments (and reminding you of upcoming ones), providing prognoses and diagnoses, referring you to other specialists or other medical practitioners and / or practices, etc.

- provide, develop and improve our medical services

- manage patient surveys and questionnaires
- check and verify your identity, and prevent, mitigate or detect and investigate crime, fraudulent or illegal activities and
- process payments.

Kindly be aware that your personal data may be processed based on more than one lawful purposes. If you need more information as to the specific legal basis on which we are relying to process your personal data, please send us your specific request to dpo@laservision.com.cy .

F. How Long we Keep your Personal Data

Personal data may be maintained by us in physical and / or electronic form and be processed in ways designed to respect the principles of purpose limitation; data minimization; data accuracy; integrity and confidentiality; and retention limitation.

Specifically with regards to retention, the technical and organizational measures operated by Laservision are designed to result in personal data being kept only for as long as required to fulfil our statutory, professional and / or regulatory obligations, and – if for longer periods - in accordance with the provisions of the specific legal basis of processing relating to each category of affected persons.

For all medical data we process, the maximum retention period is 15 years from the last interaction between Laservision and the patient.

At the end of the retention periods applicable in each case, defined operational processes or routines shall result in personal data being deleted or destroyed in controlled ways, in electronic and physical form, as appropriate. In some circumstances we may anonymise your personal information (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

G. Sharing of Personal Data

Within Laservision, your personal information can be accessed by or may be disclosed internally on a need-to-know basis, based on user access rights management processes.

Your personal information may also be accessible and / or accessed by third parties, including suppliers and advisers, as those are outlined below. When this happens, we take specific measures and steps to protect such shared information, as described in more detail in section "*Sub-Processors to Laservision*" of this Privacy Policy. In summary, such measures and steps include requiring all such 3rd parties to respect the privacy and security requirements of your personal information and to treat it in accordance with the law. We do not allow our 3rd party service providers to use your personal information for their own purposes and only permit them to process your personal information for specified purposes and in accordance with our instructions. The types of 3rd parties that may typically be involved in processing of your personal data include:

- Service providers acting as Data Processors based in the EEA such as those who provide IT, system administration services and payment providers.
- Professional advisers including lawyers, bankers, auditors and insurers based in the EEA who provide consultancy, banking, legal, insurance and accounting services.

- Tax and Customs authorities, regulators, law enforcement bodies and other authorities acting as processors or joint controllers based in the EEA who have the right to require reporting of processing activities in certain circumstances and otherwise in defense of legal claims.

- Specifically with regards to HR data, these may be shared with Payroll & Provident Fund Providers; Accountants & Auditors; Recruitment Agencies; and HCM Consultants.

In addition, there are circumstances where we may need to disclose your personal information to 3rd parties, to help manage our business and deliver our services. In this context, we may disclose your personal information:

- to 3rd parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If such a change happens to our business, then the new owners may use your personal information in the same way as set out in this Privacy Policy

- to 3rd parties when we are under a duty to disclose or share your personal information in order to comply with any legal or regulatory obligation, or in order to enforce or apply our legal rights, in which case we may share your personal information with our regulators and law enforcement agencies in the EEA, or to our legal advisers and

- when it is necessary in order to protect the rights, property, or safety of Laservision, in which case we may disclose your personal information to our legal advisers and other professional services firms.

We may also disclose your personal data to national authorities and government bodies if legislation allows or compels us to do so.

H. Categories of Personal Data Processed

As part of our operational business processes and routines and depending on the specific relationship and or commercial or other engagement in place, we may process personal data for one or more data subject categories, as those are tabulated below (not a definitive or exhaustive list).

#	Business Relationship	Type of Processed Personal Data	Legal Basis
a.	Applicants	• CV information • Contact details • Previous employment records • Referee • Clear Police / Criminal Record • Work permit information • Skills & Professional and Academic Achievements (e.g. languages, academic degrees) • Medical information (for specific vacancies / jobs only)	Consent Legitimate Interest (for application information voluntarily submitted by the applicant to us, unsolicited by Laservision
b.	Employees, Contractors & Workers	• "Master Data" [full name, ID, Social Security number, address, marital status, children, age, gender, personal emails] • "Recruitment Data" [academic records, experience, previous employers, references]	Contract

#	Business Relationship	Type of Processed Personal Data	Legal Basis
		• Evaluation & Performance Information [salary, appraisals, promotions, disciplinary data, complaints and resulting investigations, appeals against HR decisions] • Occupational data [languages, special skills, driver license] • Operational data [sales, locations of travel, training records, leave of absence, timesheets / arrival and departure times, passports and IDs in support of business travel arrangements] • Financial data [payroll, payroll-related, life insurance details, family status, bank account details]	
c.	Former Employees, Contractors and Workers	For former employees, contractors or workers, the personal data types listed in (b) above are processed with the following differences: • Financial data are kept for a period of 12 years after termination or resignation, for tax and regulatory purposes • All other data are kept for a period of 3 years after resignation or termination for the purposes of archiving and / or providing references	Employment and Social Insurance Legislation Employment / Work Contracts
d.	Patients (including children)	In the context of patient personal data processing, by Laservision, the following personal data is processed: • Full name • Gender • Age and birthday • Mobile, work and home phone numbers • Location information (physical address and electronic location data), home, delivery, work • Electronic identifiers such as IP addresses, usernames, emojis • Identification numbers such as National IDs, Passports, Driver Licenses • Economic (such as previous medical fees charged for visitations, operations, etc.) • Physiological such as height, weight, complexion, eye or hair colour, allergies, etc. (which under GDPR are special categories, and for which specific measures are operated to establish a valid, legal basis of processing) • Cultural or data defining social habits or identity (which under GDPR are special categories, and for which specific measures are operated to establish a valid, legal basis of processing) • Current and prior medical conditions and other pertinent medical information such as scans, to	Consent Legitimate Interest

#	Business Relationship	Type of Processed Personal Data	Legal Basis
		facilitate prognoses and diagnoses, medical prescriptions and treatments, etc.	
e.	Suppliers and subcontractors	The information listed below relates to business to business relationships between Laservision and its suppliers, which includes, results or requires personal data processing of Directors, Officers and personnel of Laservision's suppliers' personnel involved in the relationship, as well as other physical persons who have responsibility for managing or executing dealings between the two parties. • Identify and position / role information • Location information (physical address and electronic location data) • Business eMail address and phone numbers • Mobile phone numbers (corporate or personal) • Authority to place orders, make financial inquiries, execute financial transactions, etc. • Vetting data (in specific cases only)	Contract Legitimate Interest
f.	Onsite Visitors & Guests	• Full name • Employer • Person(s) to visit • Camera / CCTV recordings	Legitimate Interest
g.	General Public	• Full name, eMail, phone numbers, employer, title (for cases where you initiate an electronic communication and / or correspondence with us) • Photos and images of you from CCTV cameras we operate • Vehicle registration number (in case you use Laservision's parking lot)	Legitimate Interest
h.	Website Users	• Full name • Gender • eMail address (business or personal) • Mobile, and work phone numbers • Location information (physical address and electronic location data) • Electronic identifiers such as IP addresses, usernames, emojis	Consent Contract (where this information is collected for the purpose of entering into a contract with you)

I. Technical & Organisational Measures Protecting Personal Data

GDPR imposes obligations to Data Controllers and Data Processors which are in several cases dependent upon consistent implementation of relevant measures and controls across their own operations as well as those of their Data Processors. Our policy is to process personal data with due regard to the security, privacy and protection of the data we receive, store and process. This privacy policy explains the types of such technical and organizational measures that we employ so as to enhance the level of protection of personal data that we process. These measures are also designed to maximise the control over privacy in accordance to GDPR and have the objective of providing a level of security that is appropriate to the related risks.

- As part of our overall data protection framework, [customer] has appointed a Data Protection Officer (DPO), in accordance with the requirements of GDPR. Our DPO can be contacted at dpo@laservision.com.cy .
- All our personnel, including Doctors, nurses and administrative staff periodically observe GDPR-specific awareness sessions so as to maintain the currency of their understanding of GDPR and privacy and how it may impact our various operations that affect personals data we process.
- We seek to ensure that 3rd parties who support Laservision operations or systems or who are otherwise involved in our personal data processing operations (including those of our patients, employees or other affected persons), have and operate necessary technical and organizational measures for protecting the security and privacy of personal data.
- Our Incident Response Management and breach notification procedures, are designed to include escalation of identified incidents to our Data Protection Officer, who is authorized and trained to involve designated personnel of Laservision when such incidents involve personal data processed by Laservision.
- Our processes are designed not to allow cross-border data transfers of personal information to which we have access and / or process during any customer engagement. If such cross-border data transfers are necessary, we shall seek to ensure that a valid lawful basis for such transfers evidently exists, in accordance with GDPR.
- Our recruitment and ongoing personnel training and development, as well as the evaluation and disciplinary processes we operate, are designed to promote and maintain a high standard of professional ethics and competency at all levels of Laservision, which is in line with industry standards and our professional and legal responsibilities.
- In addition, Laservision operates several complementary technical and organisational measures, designed to protect the privacy of personal information that we collect, store and process. Such measures include logical access controls and user rights management with the objective of minimising access to personal (and other patient information and data, only to authorised Laservision personnel. We also utilise user access credentials management with enforced frequent changes, password complexity and maximum / minimum lengths, restrictions on reuse of same passwords, etc., complemented by a structured process for periodic review and confirmation of continued business need to such personal data.
- Furthermore, Laservision uses purpose-specific technologies and tools (such as firewalls, intrusion prevention, mail security gateways, etc.), all designed to monitor and manage the security of its electronic perimeter.

- A part of our operations involves 3rd parties (legal or physical persons) who are involved and / or provide support in many aspects including invariably in personal data processing. The related technical and organizational measures which we apply and operate with the objective of enhancing and maintaining privacy are described in the next section.

J. Sub-Processors to Laservision

Like almost all organizations, Laservision utilizes 3rd parties as part of its business operations and routines. Such 3rd parties include legal and / or physical persons who provide services and / or products relating to technology, facilities management, legal and other areas which may have an impact on personal data processing (including processing as specified in this Privacy Policy).

When necessary in the context of such personal data processing, our selection process and criteria for cooperation with 3rd parties (suppliers, vendors or other advisors), incorporates consideration and evaluation of those 3rd parties' level of GDPR readiness and compliance. In this respect, we seek to ensure that 3rd parties who support Laservision operations or systems or who are otherwise involved in our personal data processing operations, have and operate necessary technical and organizational measures for protecting the security and privacy of personal data. Whenever relevant therefore, our contracts with 3rd parties include specific provisions designed to

- identify the respective role of the 3rd party as a Data Processor or Sub-processor to Laservision
- define the 3rd party's GDPR-related obligations towards Laservision, including:
  - ✓ enforcement of Laservision's Data Retention Periods
  - ✓ integration of the 3rd party's Incident Response Management Process into that of Laservision
  - ✓ stipulating allowable access and connectivity methods for remote support (where relevant and necessary)
  - ✓ definition of the processes via which Laservision shall issue relevant instructions to the 3rd party in relation to the expected and required processing of personal information (where applicable), under each respective agreement
  - ✓ stipulation of the technical protection methods and treatment of software system replicas (for example for QA and / or development purposes) by the 3rd party, such as encryption and / or pseudonomisation of personal data
  - ✓ prohibition for conducting cross border data transfers by the 3rd party, except with the express, prior written permission of Laservision (which itself is subject to, must be in line with and in compliance to, Laservision's obligations to affected data subjects).
- conferring to Laservision the right to conduct periodic audits (including surprise audits) against the execution of GDPR related processes which the 3rd party supports and / or operates on Laservision's behalf. In this context, Laservision also seeks to implement review processes with the 3rd party Data Processors or sub-processors so as to jointly monitor on a periodic basis the effectiveness of execution of privacy processes and routines, in order for such processes to become and continue to be "Private by Design", as relevant.

K. Your Rights

Individuals whose data are processed, have defined rights under the GDPR. Specifically, GDPR requires Data Controllers and Data Processors to implement the necessary processes and mechanisms in support of data subjects' exercising the following rights, the exact definitions of which have the meanings assigned to them by the GDPR:

- Right to information as to the personal data processing being performed and the rationale of such processing
- Right to access to the personal data being processed for his / her person
- Right to rectification allowing individuals to request the correction or amendment of their data
- Right to object to a specific type of processing, under specific circumstances
- Right to object to automated processing or profiling in cases where automated processing results in decisions that in the opinion of the affected data subject, do not adequately reflect the unique characteristics of the case involved
- Right to withdraw consent allowing a data subject to give notice and withdraw a previously given consent for a specific type of processing
- Right to data portability allowing the transfer of personal data processed by a Data Controller to the data subject or directly to another Data Controller in electronic, machine readable format
- Right of Erasure ("right to be forgotten") entitling a data subject – under certain circumstances - to request the deletion of their personal data.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights as listed above). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. In extreme cases, we may even refuse to comply with your request in such circumstances.

L. Queries & Complaints

Laservision is committed to acknowledge, consider and respond to all queries and complaints that it receives from any natural person who believes is affected by Laservision's processing of his / her data. To communicate such queries or complaints please contact us on dpo@laservision.com.cy, and we shall seek to respond to the substance of your query as soon as practical, within a 30 day window as stipulated by GDPR.

If despite our responses and actions to address your concerns, you are not satisfied, you have the right to address the matter to the Cyprus Data Protection Commissioner whose offices are at Jason street 1, 2nd Floor, Nicosia 1082. The Commissioner's office can be reached on +357 22818456 and their email address is commissioner@dataprotection.gov.cy.

M. Other Important Information

This Privacy Policy does not alter in any way other than explicitly defined herein, the obligations and responsibilities of Laservision or its patients, employees, vendors or partners, all of which are governed by the respective contracts (where applicable) and / or related arrangements between Laservision and each of those patients, employees, vendors or partners.

N. Other Important Information

Our Data Protection Officer details are as follows:

PHOENIXPRO Ltd
Georgios A. Korellis
dpo@laservision.com.cy
+357 22677007.

O. Glossary & Useful Definitions

#	Term	Definition
1.	Personal Data	Also referred to as "personally identifiable information (or "PII"), personal data is any information relating to an identified or identifiable living natural person (the "data subject")
2.	Legal Basis of Processing	The basis on which the processing of personal data may be based and may be one of the following: • the consent of the data subject to the processing of his / her personal data • processing is necessary in order to enter into a contract to which the data subject is a contractual party or to take action at the request of the data subject before or after a contract is entered into force • processing is necessary to comply with a statutory obligation of the Data Controller or the Data Processor as the case may be • processing is necessary for the purposes of the legitimate interests pursued by the Data Controller, unless such interest overrides the interest or fundamental rights and freedoms of the data subject who require the protection of personal data, in particular if the subject of the data is a child • processing is necessary to safeguard the vital interest of the data subject or other natural person • processing is necessary for the performance of an obligation performed in the public interest or in the exercise of public authority assigned to the Company.

#	Term	Definition
3.	Legitimate Interest	Our lawful interests in conducting and managing our business to enable us to give you the best services and / or products and secure and private by design experience. In choosing to perform personal data processing under the legal basis of legitimate interest, we seek to ensure that we consider and balance any potential impact on you (both positive and negative) and your rights before doing so. As a general principle, we do not use your personal information for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).
4.	Data Controller	The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.
5.	Data Processor	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.
6.	Data Protection Officer	A Data Protection Officer (or "DPO") is a privacy leadership role required by the GDPR. The DPO is responsible for (a) overseeing data protection strategy and implementation within an organization; (b) ensuring compliance with GDPR requirements; (c) the provision of advice to the Data Controller or the Data Processor and their staff in relation to personal data processing; and (d) to cooperate with Data Protection Authorities and supervisory bodies in all privacy and data protection matters.
7.	Cross-border Data Transfers	Transfers of personal data outside the European Economic Area in physical and / or electronic form