Personal Data Protection Policy

Introduction

We, VISIONIX - Luneau Technology Operations, a simplified joint-stock company, registered on the Trade Registry of Évreux, under SIREN (business reg.) number 08615020800048, whose registered office is located at 2 rue Roger Bonnet, 27340, Pont de l'arche, offer ophthalmology equipment and services to eye health professionals.

Within the framework of our business, we have to collect, transmit and/or store personal data. However, the security and privacy of this data, which may be particularly sensitive in nature due to our sector of activity, is of the utmost importance to us.

As such, we guarantee that we comply with the applicable personal data protection regulations and in particular Regulation EU 2016/679 of 27 April 2016: The General Data Protection Regulation (hereinafter the "GDPR"). We undertake to ensure that:

- You retain control over your personal data;
- Only data that is strictly necessary is collected and processed;
- The data is collected in a transparent, confidential and secure manner.

In order to ensure these rules are applied properly, we have appointed a DPO, your point of contact should you have any queries about this privacy policy, and they are the dedicated point of contact of the Supervisory Authority for the protection of personal data.

In the interests of transparency and fairness, this Personal Data Protection Policy (hereinafter the "Policy") explains why and how we process your data.

We understand that reading this type of document can be tedious, **but we urge you to read it in full.** For more information and transparency, its key elements are summarised in the outline below:

Definitions

Firstly, here are some definitions of the terms used in this document:

Medical device*:* any instrument, appliance, equipment, software, implant, reagent, material or other item, intended by the manufacturer to be used, alone or in combination, by humans for one or more of the medical purposes outlined in Article 2 of REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 concerning medical devices.

Personal data (hereinafter "Data"): any information that identifies a natural person directly (e.g. last name/first name), or indirectly (such as a contract number/telephone number/IP address).

Sensitive data: information about race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used to identify a natural person personally, data about health, sex life or sexual orientation. This data is subject to enhanced protection based on the principle that it may not be collected or processed. However, it is possible to get around this prohibition by means of a number of exceptions set out in Article 9.2 of the GDPR (including consent).

Healt-related data: data about the past, present or future physical or mental health of a natural person (including the provision of healthcare services) which reveals information about the state of that person's health. This notion includes health data by its very nature (medical), but also data which, when combined or cross-referenced with other data, becomes health data, meaning it enables a conclusion to be drawn about a person's health. Or data which, because of its intended use, becomes health data (e.g. photo of a physical feature used by a surgeon to perform an operation). This includes information collected about a person when they register to receive healthcare services or during the provision of said services.

Data Processing: operation or set of organised operations performed on the Data (viewing, collection, structuring, analysis, retention, modification, transmission, etc.)

Data Controller: the person who determines the purposes and the means of the processing, what your Data will be used for and what tools will be used to process this Data.

Data Processor: the person that carries out the operations on the Data on behalf of and in accordance with the instructions of the Data Controller.

Recipient: the person who receives the authorised disclosure of the Data.

User: any person who uses our Visionix Solutions. Users may be Operators or Eye Care Provider.

Customer: User who subscribes to one of our offers on the e-commerce platform.

Data Protection Officer ("DPO"): the person appointed by the Data Controller to monitor compliance with the protection of personal data it processes in accordance with the provisions of the GDPR.

Scope of the Policy

This Policy applies as soon as you use one of the following Visionix solutions:

- **Visionix EyeRefract**: Class IIa medical device which guides the operator through each stage of the physiological refraction process of the patient's eye.

- **Visionix VX650**: Class IIa medical device which provides a comprehensive examination of the patient's eye to detect and monitor the main eye conditions and facilitates the assignment of tasks.

- **Nexus**: A digital health platform designed to connect all eyecare professionals, even remotely/database collected in encrypted form by medical devices and stored by an HDS-certified host (Health Data Hosting).

The medical devices linked to Nexus make it possible to provide the expertise of eyecare professionals to patients, even remotely, in any eye testing facility.

You Data is also processed via the **Visionix e-commerce platform**, through which you can sign up to the Nexus Platform and purchase credit to use the Visionix Solutions. This platform also facilitates the payment of Users involved in providing services to the patient.

This Policy is subject to the acceptance of our Terms and Conditions of Use and Terms and Conditions of Sale and it is brought to your attention when you create your Nexus account and/or take out your licence and purchase credits.

The processing of sensitive data and/or Health-related data is only carried out after the consent of the data subjects has been obtained.

Who is the Data Controller?

When you create your user accounts on our platforms, VISIONIX – Luneau Technology Operations is the Data Controller.

When you sign up to the Nexus Platform or purchase user credits, VISIONIX – Luneau Technology Operations is also the Data Controller.

When you use one of our Visionix Solutions: VISIONIX – Luneau Technology Operations is the Data Controller for the Data required to manage your use in accordance with the Terms and Conditions of Use of its Solutions. In particular regarding the maintenance and security of its Solutions. It is also the Data Controller for the processing operations carried out to meet its legal obligations covering Medical Devices.

VISIONIX – Luneau Technology Operations also acts as a Data Processor for data processing operations carried out on behalf of and in accordance with the instructions:

- Of the Operator: to establish contact with the Doctor, to transmit the information required to perform the actions it is authorised to perform in terms of eyesight correction, and to monitor these actions, and pay the Doctor.
- Of the Eye Care Provider: for the purposes of establishing contact with the Operator and with the patient, for the purposes of monitoring grading requests, assessment for the purposes of prescribing visual correction, screening and medical monitoring, in particular by collecting the information required for its analysis.

In order to gain a better understanding, we will detail the purposes for which we use your data as the Data Controller in the following article.

Why do we use your Data?

In order to process personal data, this processing must be based on one of the reasons permitted by law, a “legal basis”. Below, we outline the purposes for which we use your Data and what gives us the right to process this Data.

PURPOSES	**LEGAL BASIS**
Management of users of the Nexus Platform (creation and management of accounts)	GDPR Article 6.b): Contractual fulfilment
Technical management of the platforms (maintenance and technical assistance)	GDPR Article 6.b): Contractual fulfilment
Management of the security of the Nexus Platform (HDS) and our Information Systems	GDPR Article 6.c): Legal obligation GDPR Article 6.f): Legitimate interest
Management of our partnerships with Users	GDPR Article 6.b): Contractual fulfilment and pre-contractual measures
Improvement and development of our products and services (including User statistics)	GDPR Article 6.f): Legitimate interest
Accounting and contractual management of our Customers	GDPR Article 6.b): Contractual fulfilment, GDPR Article 6.c): legal obligation
Carrying out analyses and statistics that do not enable direct identification to monitor our medical device.	GDPR Article 6.c): Compliance with our legal obligations in terms of monitoring our Medical Devices
Research and development (in particular to develop and validate algorithms used as part of our activity)	GDPR Article 6.f): Legitimate interest + GDPR Article 9.2.b) (patient consent for sensitive data)
Management of our Records and procedures linked to the management of your rights and protection of your data	GDPR Article 6.f): Legitimate interest GDPR Article 6.c): Legal obligation

PURPOSES	LEGAL BASIS
Management of complaints, management of disputes, exercise or defence of a right in court	GDPR Article 6.f): Legitimate interest

What Data do we use?

- **Operator Data:**

Identification Data, including: Last name*, First name*, postal address*, email address, telephone number, login details (we cannot see the unencrypted password).
Connection data, including: IP address, connection log on the platforms
Data about your professional life: Profession, company name*.
Miscellaneous: Nexus account preferences, data relating to subscriptions and purchases of credit (date, type of purchase, number of credits, etc.)

- **Doctor Data:**

Identification Data, including: Last name*, First name*, postal address*, email address, telephone number, login details (we cannot see the unencrypted password).
Connection data, including: IP address (when associated with a freelance doctor), connection log on the Nexus platform.
Data about your professional life: Profession, licence number, Code
Miscellaneous: Nexus account preferences

- **Patient's Data:**

For Optician /Doctor purposes:
Personal Information are entered by the Optician into the Visionix Solutions: first Name*, last Name*, birth date*, gender*, country, city, internal code,

Sensitive data collected by using Visionix Solutions: it may include patients' ethnicity (important information in the field of visual health), Heath-related data (measurements enabling the lens correction formula to be defined, posterior and anterior measurements of the eye enabling the doctor to detect any diseases).

Personal information such as name, email address, and contact information in order to provide patients with access to the Platform and to communicate with patients about their use of the Platform.

Additional personal information such as medical history, and Health-related information if patients choose to provide it to their Optician.

- **For Visionix – Luneau Technology Operations purposes:**

Patient ID, birth date, ethnicity if applicable, gender, measurements enabling a lens correction formula, posterior and anterior measurements of the eye.

Who are the recipients of this Data?

Only the specific and authorised individuals mentioned below may have access to your Data:

- The authorised staff of VISIONIX
- Patients
- The User involved in performing tasks
- VISIONIX data processors, for example the website host, within the strict framework of their assignments and in accordance with the requirements of the GDPR, in particular in terms of security and privacy.
- The relevant public authorities, in accordance with the regulations, in the event of a request (provision, if necessary).

We would like to point out that we have selected, as an HDS-certified health data hosting company:

AWS - Frankfurt

EUROPE (FRANKFURT)	For security reasons, DC physical addresses are not provided by Amazon Web Services

Your Data is not disclosed, exchanged, sold or leased to any other person.

All Data destined for the host is encrypted in advance.

Data retention period

We undertake to retain your data for the duration **strictly necessary** for the purposes for which the data was collected and processed.

In order to define these periods, we refer to the legal provisions in force, to any statutes of limitations and to the recommendations/benchmarks of the Supervisory Authority in terms of personal data protection.

For example, we retain:

- Data relating to the exercise of one of your GDPR rights under this Policy: 5 years from the expiry of the response period.
- Data relating to our contractual relations: the term of the contractual relations, plus 5 years from the end of the contract for evidential purposes or to comply with a legal obligation.

- Data required to comply with our accounting and tax obligations: 10 years.

Transfers of data outside the EU

We take particular care to select solutions and subcontractors that are GDPR-compliant. When processing your Data, VISIONIX uses partners located outside the European Union, but the Data is managed and stored in Europe.

Any transfers outside the EU are carried out under the supervision of our Data Protection Officer (DPO), who ensures that these transfers are lawful by assessing the appropriate guarantees proposed by the data processors, and the measures to be implemented to ensure an adequate level and suitable level of protection in terms of data security and privacy, in accordance with the Regulations in force.

What are your rights?

In accordance with the Regulations in force, you have the right to access, rectify, and erase (subject to conditions) your data, as well as the right to data portability (for processing operations based on consent or contractual fulfilment), the right to restrict the processing of your data and the right to determine the fate of your data after your death.

Here is a table summarising your rights and what they entail, depending on the legal basis for processing:

GDPR rights	**Consent**	**Contractual fulfilment**	**Legitimate interest**	**Legal obligation**
Right to access: the right to obtain the information listed in GDPR article 15, and a copy of the data that has been processed.	✓	✓	✓	✓
Right to rectify: the right to rectify inaccurate or incomplete data that you cannot update yourself (GDPR article 16)	✓	✓	✓	✓
The right to erase/be forgotten: data that is inaccurate, incomplete, ambiguous, out-of-date or whose collection/use is not or no longer lawful (GDPR article 17)	✓	✓	✓	
Right to object: the right to object to the processing of your data			✓	

GDPR rights	Consent	Contractual fulfilment	Legitimate interest	Legal obligation
under the conditions outlined in GDPR article 21				
Right to withdraw your consent (GDPR article 13.2.c)) at any time (in the future)	✓			
Right to restrict: the right to request a temporary freezing of your data (marking to limit future processing of your data), in the 4 cases outlined in GDPR article 18	✓	✓	✓	✓
Right to data portability (GDPR article 20) : the right to request part of your data (collected directly, processed automatically, insofar as this does not infringe the rights of a third party, if their data is included) in an open and machine-readable format	✓	✓		

You also have the right to object, at any time, for reasons pertaining to your specific situation, for processing operations based on legitimate interest.

You also have the right to lodge a complaint with the relevant Supervisory Authority at the following address:

How can you exercise these rights?

To exercise these rights, please send a request to our DPO:

Either by email: **dpo@visionix.com**
Or by post:
Société VISIONIX,
DPO,
2 rue Roger Bonnet, 27340, Pont de l'arche, France

Please include:

- Your contact details (last name, first name, address)
- The reasons specific to your particular situation when required by law (in particular in the event you object to processing based on legitimate interest)
- The legal basis in the event you are exercising the right to erase your data.

We may request a copy of your identity document to prove your identity and this may be retained for the time required to verify your request or comply with a legal obligation.

We will reply to you within 1 to 3 months of receipt of your request.

Security measures

Data security refers to the measures taken to protect your data from the following:

- Alteration
- Destruction
- Loss
- Disclosure or unauthorised access

To ensure an adequate level of security for the risks involved, right from the design phase, we must implement the appropriate technical, legal and operational measures, given our current understanding of , and the nature, scope, context and purposes of the processing operations.

As such, we implement the following measures:

- Appointment of a Data Protection Officer (DPO)
- Performance of privacy impact assessments
- Authentication processes with personal and secure access
- Measures aimed at ensuring the privacy, integrity, availability and resilience of our information systems, including:
    - daily data and infrastructure back-up processes,
    - secure HTTPS connection
    - software: firewall, virus protection
    - Encryption
    - Pseudonymization

Updates

This policy may be amended or modified at any time in the event of changes to legislation, case law, decisions and recommendations of the Supervisory Authority in terms of personal data protection, or practices.

In the event of significant updates or amendments to this Policy, we undertakes to inform you in advance of the implementation of amendments that may have an impact on the processing of your personal data.

We undertake to clearly indicate the date of the update and the latest version of this Policy.