Privacy notice for NOVA SOFTWARE

The Nova platform is a software solution to enable opticians and eyewear retailers to collect information about their customers listed below. In order to ensure that this personal data is collected in compliance with the law, Optinet Limited is providing this privacy notice about the Nova platform and how personal data is processed by opticians (who are the controllers of the personal data they collect about their customers and clients using the Nova platform. The Nova platform is a management platform and includes managing the following functions :

- Patient records
- Recalls
- Appointments
- Clinical
- Dispensing
- Till
- Schemes
- Orders
- Stock
- EGOS
- Management reporting
- Internal messaging / tasks

The data that may be collected and stored on the Nova Platform

Opticians may upload different kinds of personal data about their clients onto the Nova platform, including:

- Identity Data : first name, surname, DOB
- Patient Data : NHS number, appointment times and dates, appointment history, test and services provided during appointments, relevant medical history
- Contact Data : first name, surname, email addresses and telephone numbers, postal addresses
- Financial Data : Bank details for direct debit collection
- Transaction Data: appointments made and attended, services provided or booked, products bought or ordered
- Profile Data : transaction data, identity data and contact data
- Marketing and Communications Data: profile data adapted to create marketing lists for different products or services that are directed only at those clients who have requested information or have previously used the service (or a very similar service) or bought the product (or a very similar product).

Typically, using the Nova platform, an account is created by the optician retailer for an individual client, which enables the optician retailer to store and access the information relating to the client for each repeat visit; this can assist in the quality and continuity of service provided to the client in person and can also provide the optician retailer with the contact data to enable them to send relevant permitted marketing to the client,

tailored to be of interest to the client. In order to use the Nova platform fully and compliantly with data protection laws, the data controller (optician retailer) must provide information about how the Nova platform processes personal data. This can be done by including information from this product specific privacy notice to data subjects adding it to the opticians own general privacy policy.

Each optician retailer can set the retention periods and review or audit dates for their own use of the Nova platform, and these should be notified to the data subjects in the opticians general privacy policy.

All personal data uploaded on to Nova Software is stored in the UK on ANS and AWS servers, benefitting from their state of the art systems and industry best practice security to protect data subjects personal data. There is no transfer of personal data out of the EEA or the UK as a result of uploading personal data to the Nova platform.

The Nova platform relies on the following third parties to provide support services (and so these third parties will process some of the personal data uploaded on the Nova Software in order only to provide the support services to Optinet Limited):

- CFH Docmail
- ANS
- AWS
- 24X
- GBG Plc
- Bottomline Technologies
- SMTP2Go
- PCSE
- ATOS

The Nova platform includes the following security features :

Physical access controls

- Nova servers are virtual and located within an ANS data centre (Tier 3)
- Access to the console for these virtual servers requires
  - Username / password
  - 2-factor authentication
- Office based devices storing private keys for use in authentication have encrypted drives

System access controls.

- Access to the optician retailer’s control system:
  - username / password
  - requires 2-factor authentication
- User devices that access Nova:

- Username and password
- Whitelisted devices only
- Device whitelisting is via 2-factor authentication

Data access controls.

- Access to the data is only available to authorised Optinet staff
  - Access via SSH connection only
  - Username / password
  - Public key cryptography for authentication

Transmission controls.

- Connections to the application are secured via SSL
- http connections are disallowed - only https are allowed.
- Data transferred to Optinet is secured via SSL and only used on encrypted devices

Input controls.

- Data is validated at time of submission
- Application data requests are processed by the Eloquent ORM and are sanitised to protect from SQL injection

Data backups.

- Full data backup is performed once per day
  - Backups are retained for 7 days
  - Backups are stored off-site
  - Access to offsite storage requires 2-factor authentication
- Data is replicated from Live server to Slave server continuously
- Server images are backed up within the data centre

Data segregation.

- Each optician retailer uses their own sub-domain and has a distinct set of user accounts
- Each optician retailer's data is stored in a separate database