4 Sight Opticians General Data Protection Regulation (GDPR)

Privacy Notice for Patients & Customers

We issue this privacy notice in the interests of transparency over how we use ("**process**") the personal data that we collect from patients and customers.

Personal data for these purposes means any information relating to an identified or identifiable person.

"**Sensitive personal data**" means personal data consisting of information as to -

a) the racial or ethnic origin of the individual,
b) their political opinions,
c) their religious or philosophical beliefs,
d) their membership of a trade union,
e) their physical or mental health or condition,
f) their sexual life,
g) the commission or alleged commission by them of any offence,
h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings,
i) genetic data; and
j) biometric data where processed to uniquely identify a person (for example a photo in an electronic passport)

Data Controller

For data protection purposes the "**data controller**" means the person or organisation who determines the purposes for which and the manner in which any personal data are processed.

The data controllers are Rod Mason and Nigel Atkinson, 4 Sight Eyecare Centres Ltd, 5 Hollies Court, Hollies Park Road, Cannock, WS11 1DB (Head Office).

Purpose of processing the data

It is necessary for us to obtain and process personal data of Customers and Patients for the following reasons:

1. We will need the information for the purpose of carrying out eye examinations and providing associated services;

2. We will need to maintain that information for the general purposes of any ongoing commercial relationship and clinical patient data will be maintained in accordance with prevailing legislative requirements.

Our legal basis for processing personal data Customers and Patients is that:

1. Processing personal data is necessary to identify the individual for the purposes of clinical record keeping, generating appointment reminders and obtaining payment for goods or services supplied;

2. Processing is necessary to comply with legal obligations (for example we are obliged to keep clinical records for a minimum of 7 years or longer in the case of children) and commercial purposes;

3. Processing the data is necessary for the purposes of our "**legitimate interests**" as the data controller (except where such interests are overridden by the interests, rights or freedoms of the individual).

Our "legitimate interests" for these purposes are:

1. the need to process data on customers or patients for the purposes of assessing eligibility for both private and NHS eyecare services;

2. the need to gather data for the purposes safeguarding in compliance with statutory requirements;

3. the need to transfer customer or patient data intra-group for administrative purposes; and

4. notification that recommended appointments are due (or overdue), sending appointment reminders, order ready for collection notifications and permitted marketing activities.

We may from time to time need to process sensitive personal data, for example medical records or other information relating to the health and well being of an individual.

In that case we will either obtain the explicit consent of the individual to the processing of such data or we may consider the processing of that data as being necessary for carrying out our obligations as a provider of eyecare services. That will be assessed on a case by case basis.

There is no strict statutory or contractual requirement for you to provide data to us but if you do not provide at least that data that is necessary for us to assess eligibility it may not be possible for us to provide you with the eyecare and associated services that we offer. This may include any relevant medical history and details of treatments or eyecare products previously carried out or supplied to you.

Recipients of personal data

Your personal data may be received by the following categories of people:

1. Our Head Office Department
2. Your appointed bank if payments are made by Direct Debit
3. Any individual authorised by us to maintain personnel files including;
4. Our appointed Practice Management System providers
5. Our appointed mailing house and or marketing organisation.
6. For drivers of vehicles in some cases; the DVLA and appropriate external authorities.
7. Our professional advisers such as insurance and legal advisors;
8. Appropriate external regulators and authorities such as NHS administrative bodies.
9. Your General Practitioner and/or Private medical insurers if applicable.
10. Professional bodies such as AOP, ADO, BCO and GOC where applicable.
11. Our appointed manufacturers and suppliers of optical goods and services.

Where personal data is transferred to any of the above, it is done so according to a contractual agreement between the controller and processor. As per this agreement personal information is securely stored within the EU and is not sold to third parties.

We do not envisage that your data would be transferred to a third-party country. If we perceive the need to do that we would discuss that with you and explain the legal basis for the transfer of the data at that stage.

Duration of storage of personal data

We will keep personal data for no longer than is strictly necessary, having regard to the original purpose for which the data was processed.

In some cases we will be legally obliged to keep your data for a set period. For example we are obliged to keep clinical records for a minimum of 7 years (or longer in the case of children) from the date of the most recent appointment.

If paying by Direct Debit your data will be kept for the duration of any ongoing transactions plus a reasonable period following cessation of any payments and/or agreements.

Your rights in relation to your personal data

1. The right to be forgotten

You have the right to request that your personal data is deleted if:

a) it is no longer necessary for us to store that data having regard to the purposes for which it was originally collected; or
b) in circumstances where we rely solely on your consent to process the data (and have no other legal basis for processing the data), you withdraw your consent to the data being processed; or
c) you object to the processing of the data for good reasons which are not overridden by another compelling reason for us to retain the data; or
d) the data was unlawfully processed; or
e) the data needs to be deleted to comply with a legal obligation.

However, we can refuse to comply with a request to delete your personal data where we process that data:

a) to exercise the right of freedom of expression and information;
b) to comply with a legal obligation or the performance of a public interest task or exercise of official authority;
c) for pubic health purposes in the public interest;
d) for archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
e) the exercise or defence of legal claims.

2. The right to data portability

You have the right to receive the personal data which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided (us) where:

a) the processing is based on consent or on a contract; and

b) the processing is carried out by automated means.

Note that this right only applies if the processing is carried out by "automated means" which means it will not apply to most paper based data.

3. The right to withdraw consent

Where we process your personal data in reliance on your consent to that processing, you have the right to withdraw that consent at any time. You may do this in writing to our Head Office.

4. The right to object to processing

Where we process your personal data for the performance of a legal task or in view of our legitimate interests you have the right to object on "grounds relating to your particular situation". If you wish to object to the processing of your personal data you should do so in writing to our Head Office stating the reasons for your objection.

Where you exercise your right to object we must stop processing the personal data unless:

- we can demonstrate compelling legitimate grounds for the processing, which override your interests, rights and freedoms; or
- the processing is for the establishment, exercise or defence of legal claims.

5. The right of subject access

   So that you are aware of the personal data we hold on you, you have the right to request access to that data. This is sometimes referred to as making a "subject access request".

6. The right to rectification

   If any of the personal data we hold on you is inaccurate or incomplete, you have the right to have any errors rectified.

   Where we do not take action in response to a request for rectification you have the right to complain about that to the Information Commissioner's Office.

7. The right to restrict processing

   In certain prescribed circumstances, such as where you have contested the accuracy of the personal data we hold on you, you have the right to block or suppress the further processing of your personal data.

8. Rights related to automated decision making and profiling

   The GDPR defines "profiling" as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict:

   - performance at work;
   - economic situation;
   - health;
   - personal preferences;
   - reliability;
   - behaviour;
   - location; or
   - movement

You have the right not to be subject to a decision when it is based on automated processing; and it produces a legal effect or a similarly significant effect on you.

However, that right does not apply where the decision is necessary for purposes of the performance of a contract between you and us. We may use data related to your performance or attendance record to make a decision as to whether to take disciplinary action. We consider that to be necessary for the purposes of conducting the employment contract. In any event that is unlikely to be an automated decision in that action will not normally be taken without an appropriate manager discussing the matter with you first and then deciding whether the data reveals information such that formal action needs to be taken. In other words there will be "human intervention" for the purposes of the GDPR and you will have the chance to express your point of view, have the decision explained to you and an opportunity to challenge it.

Complaints

Where you take the view that your personal data are processed in a way that does not comply with the GDPR, you have a specific right to lodge a complaint with the relevant supervisory authority. The supervisory authority will then inform you of the progress and outcome of your complaint. The supervisory authority in the UK is the ICO.