

## **OPTOS PRIVACY NOTICE**

In this privacy notice we explain how we collect and use your personal data. This privacy notice applies to all personal data we process about you when you order, purchase or use our products and services, visit our websites, use our customer support or otherwise interact with Optos plc.

Optos plc respects privacy and acknowledges that processing personal data in a lawful and proper manner is an important social responsibility and declares that it will strive to protect personal data. As such we are providing this privacy notice as part of Nikon's Group Privacy Protection Statement <url: [www.nikon.co.jp/main/eng/privacy\\_policy.htm](http://www.nikon.co.jp/main/eng/privacy_policy.htm)> and applies to all personal data that we process concerning our prospective, current and former customers and suppliers (hereafter "you"), and your usage of our products and services, our Optos website at <https://www.optos.com/>, or otherwise doing business with Optos plc. In this privacy notice, we explain which personal data we collect and how we use this data. Therefore, we encourage you to read this notice carefully.

### **Contents**

- 1. Who we are**
- 2. What personal data we collect and what we do with your data**
- 3. How we collect your data**
- 4. Information sharing**
- 5. Security measures and data retention**
- 6. International transfers of personal data**
- 7. Your rights**
- 8. How we look after this policy**
- 9. Contact details for your privacy inquiries**

## 1. Who we are

We are Optos plc, (hereafter “**Optos**”) Queensferry House, Carnegie Campus, Dunfermline, Scotland KY11 8GR United Kingdom. We are part of the Nikon Group. Together with Nikon Corporation, Shinagawa Intercity Tower C, 2-15-3, Konan, Minato-ku, Tokyo, 108-6290, Japan, we are responsible for the collection and use of your personal data described in this privacy notice. References to “**Nikon**”, “**we**” and “**our**” throughout this notice, depending on the context, collectively refer to the aforementioned legal entities.

Optos plc is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

We have determined our respective responsibilities for compliance with the obligations under applicable privacy legislation for processing your personal data in relation to our global processing activities by means of an arrangement between us. In summary, we have arranged that if you want to exercise your rights, such as your right to access, correct, erase, restrict, object or port personal data or to withdraw your consent, or if you have any questions about the processing of your personal data, you can contact Optos in accordance with Section 9 Optos and Nikon Corporation will assist each other where necessary to ensure that you can exercise your rights and your questions will be handled.

## 2. What personal data we collect and what we do with your data

We have outlined our data processing operations and the purposes for which we process your personal data in the Overview of Optos processing activities in the Annex below. In summary, we use various systems to deliver products and services to you. For example, Nikon provides the following products and services: Scanning Laser Ophthalmoscopes, Optical Coherence Tomography Systems, Picture Archiving and Communication Software, Customer Service Support, Pre-Sales Business Development and Marketing and Post Marketing Device Support.

### **Sensitive data**

Some of the personal data described in the Overview in the Annex below may be considered “sensitive personal data” under applicable data protection laws. For example, the retinal image and ethnicity of a patient may qualify as sensitive data. We have outlined these data in the Overview of Optos processing activities and will only process these data in accordance with applicable data protection laws.

### **Legal basis**

Nikon processes your personal data to provide our products and services to you, to comply with legal obligations we are subject to or if it is necessary for our legitimate interests or the interests of a third party or on the basis of consent.

When we process your personal data for our legitimate interests or the interests of a third party, we will take reasonable measures to prevent unwarranted harm to you. Our legitimate interests are for example, our interest of improving our product and services delivery by storing contact details, reducing our costs, improving our newsletters and websites by analysing which parts of our communications are most relevant for you. Or of securing our services and facilities, such as the purposes mentioned in the Annex. More information on the balancing tests we perform is available upon request. Where we process your personal data for our legitimate interests or the interests of a third party, you have the right to object at any time on grounds relating to your particular situation (please see Section 7. Your rights below).

You may withdraw your consent at any time by following the specific instructions in relation to the processing for which you provided your consent, by adjusting your setting (if available) or by reaching us through the contact details in Section 9. Contact details for your privacy inquiries below.

Where we process your personal data for a purpose other than that for which we collected it initially (and we rely on a legal basis other than consent or complying with legal obligations for this new purpose), we will ascertain whether processing for this new purpose is compatible with the purpose for which the personal data were initially collected. More information on this assessment is available upon request (please see Section 7. Your rights below).

### **3. How we collect your data**

Most of the personal data we process is information that you knowingly provide to us directly or through third parties. However, in some instances, we process personal data that we are able to infer about you based on other information you provide to us or on our interactions with you, or personal data about you that we receive from a group company or a third party with or without your knowledge (please see Section 4 and the Annex below).

If you refuse to provide personal data that we require for the performance of a contract or compliance with a legal obligation, we may not be able to provide all or parts of the services you have requested from us.

### **4. Information sharing**

Optos plc, and its subsidiaries, will process some of your personal data locally. However, as a global organization, many of our business activities can also be carried out by processing or consolidating information about you in specific or centralized databases and systems located at specific secured facilities worldwide. As a result, your information may be shared with other entities within the Nikon Group. However, each Nikon Group company and those other systems and databases will only collect, receive, use, share or otherwise process such personal data in accordance with applicable laws, this privacy notice, our Nikon Group Privacy Protection Statement <url: [www.nikon.co.jp/main/eng/privacy\\_policy.htm](http://www.nikon.co.jp/main/eng/privacy_policy.htm)>. Moreover, internally we

maintain a strict access policy with regard to the processing of personal data. Only a limited group of authorized Nikon staff on a need to know basis may have access to your personal data.

As a rule, we do not share your personal data with anyone outside the Nikon Group. However, we may share your personal data with trusted third parties that perform business functions or provide services to us. All such third parties will be required to adequately safeguard your personal data, subject to agreements that correspond to the requirements of applicable laws. Your personal data may also be shared for investigations (e.g. disclosure to prevent crime or fraud, or to comply with a court order or legislation).

## **5. Security measures and data retention**

Nikon will secure your personal data in accordance with our IT and security policies so that personal data are protected against unauthorized use, unauthorized access and wrongful modifications, loss or destruction. Your personal data will be stored no longer than is necessary for the purpose they were obtained, including compliance with legal and fiscal obligations and for solving any disputes. We have outlined the specific data retention periods in the Overview of Optos processing activities in the Annex below.

## **6. International transfers of personal data**

Given the global nature of our company, your personal data may be transferred to Nikon entities and trusted third parties in countries outside the European Economic Area whose laws may not afford the same level of protection of your personal data. Where necessary, Nikon will ensure that adequate safeguards are in place to comply with the requirements for the international transfer of personal data under applicable privacy laws. For transfers of personal data outside the European Economic Area, Nikon will use Commission approved mechanisms, such as the Privacy Shield certification and Standard Contractual Clauses as safeguards, such as the “(EU-)controller to (Non-EU/EEA-)controller” Decision 2004/915//EC (see Article 46 GDPR). If you wish to receive a copy of these safeguards, please contact us through the contact details in Section 9. Contact details for your privacy inquiries below.

## **7. Your Rights**

You can contact us (please see Section 9. Contact details for your privacy inquiries below) to exercise any of the rights you are granted under applicable data protection laws, which includes (1) the right to access your data, (2) to rectify them, (3) to erase them, (4) to restrict the processing of your data, (5) the right to receiving a file of your personal data and (6) or the right to object to the processing, and where we have asked for your consent, to withdraw this consent. These rights will be limited in some situations. We will, for example, deny your request for access when necessary to protect the rights and freedoms of other individuals or refuse to delete your personal data in case the processing of such data is necessary for compliance with legal obligations. The right to data portability, for example, does not apply in case the personal

data was not provided by you or if we process the data not on the basis of your consent or for the performance of a contract.

When you would like to exercise your rights, please send your request to the contact details in Section 9. Contact details for your privacy inquiries below. Please note that we may need you to provide additional information to confirm your identity. You also have the right to lodge a complaint with the Information Commissioner's Office.

You can also contact us at if you have any questions, remarks or complaints in relation to this privacy notice.

#### 7.1. Right to access

You may ask us whether or not we process any of your personal data and, if so, receive access to that data in the form of a copy. When complying with an access request, we will also provide you with additional information, such as the purposes of the processing, the categories of personal data concerned as well as any other information necessary for you to exercise the essence of this right.

#### 7.2. Right to rectification

You have the right to have your data rectified in case of inaccuracy or incompleteness. Upon request, we will correct inaccurate personal data about you and, taking into account the purposes of the processing, complete incomplete personal data, which may include the provision of a supplementary statement.

#### 7.3. Right to erasure

You also have the right to have your personal data erased, which means the deletion of your data by us and, where possible, any other controller to whom your data has previously been made public by us. Erasure of your personal data only finds place in certain cases, prescribed by law and listed under article 17 of the General Data Protection Regulation (GDPR). This includes situations where your personal data are no longer necessary in relation to the initial purposes for which they were processed as well as situations where they were processed unlawfully. Due to the way we maintain certain services, it may take some time before backup copies are erased.

#### 7.4. Right to restriction of processing

You have the right to obtain the restriction of the processing of your personal data, which means that we suspend the processing of your data for a certain period of time. Circumstances which may give rise to this right include situations where the accuracy of your personal data was

contested but some time is needed for us to verify their (in)accuracy. This right does not prevent us from continue storing your personal data. We will inform you before the restriction is lifted.

#### 7.5. Right to receive your file (data portability)

Your right to data portability entails that you may request us to provide you with your personal data in a structured, commonly used and machine-readable format and to have such data transmitted directly to another controller, where technically feasible. Upon request and where this is technically feasible we will transmit your personal data directly to the other controller.

#### 7.6. Right to object

You also have the right to object to the processing of your personal data, which means you may request us to no longer process your personal data. This only applies in case the 'legitimate interests' ground (including profiling) constitutes the legal basis for processing (see par. 'Legal basis' above).

At any time and free of charge you can object to direct marketing purposes in case your personal data are processed for such purposes, which includes profiling purposes to the extent that it is related to such direct marketing. In case you exercise this right, we will no longer process your personal data for such purposes.

### **8. How we look after this policy**

We have most recently updated this notice on 22 May 2018 and it replaces earlier versions. We will update this privacy notice from time to time and notify you of any substantive changes.

### **9. Contact details for your privacy inquiries**

Optos plc Compliance Department  
Queensferry House, Carnegie Campus, Dunfermline, Scotland KY11 8GR United Kingdom  
[dpo@optos.com](mailto:dpo@optos.com)  
Telephone: +44 (0)1383 843350

Data Protection Officer,  
The DPO Center Ltd, 50 Liverpool Street, London, EC2M 7PY,  
[dpo@optos.com](mailto:dpo@optos.com)  
[Telephone: +44 \(0\)203 7976340](tel:+442037976340)

Alternatively, you can manage the communications that you would like to receive from Optos here: <https://www.optos.com/en/landing-pages/manage-your-email-preferences/>  
Or unsubscribe from communications here:  
<https://www.optos.com/en/landing-pages/unsubscribe/>

## OVERVIEW OF OPTOS PROCESSING ACTIVITIES

Processing operation	Categories of personal data	Special categories of personal data	Purposes	Recipients	Retention period	Further explanation and source of personal data (if applicable)
<b>Customer Service/ Repair Administration</b>	Address, Country, Email, Location data, Name, Postal Code, Phone number, IP Address	Health and Medical	Patient data can be visible or retained on device during service or replacement process	Service Providers	Life of Device + 2 years	
<b>End Customer Administration</b>	Address, Country, Email, Location data, Postal Code, Name, Phone number, IP Address		Customer relationship:	Regulatory Auditors, Supplier Correspondence	Life of Device + 2 years	
<b>Customer Service/ Repair Administration</b>	Address, Country, Email, Location data, Postal Code, Name, Phone number, IP Address		Administration, Compliance with law, Customer relationship, Regulatory Reporting	FDA MHRA MHLW Health Canada Taiwan All Relevant Regulatory Bodies	Life of Device + 2 years	Customer Service Rep Field Service Engineers Distributors, Contracted Service Providers
<b>Vendor Administration</b>	Address, Country, Email, Location data, Postal Code, Name, Phone number, IP Address		Administration, Compliance with law, Customer relationship, Contract execution, Vendor Management:	authorized employees Regulatory Auditors,	Life of Device + 5 Years	Credit Check Suppliers and Lawyers
<b>Others Prospective Customer Data</b>	Address, Country, Email, Location data, Postal Code, Name, Phone number,	Professional Body Registration	Direct Marketing	Regulatory Auditors, Transferred to external 3rd party servers	CET - 7 Years/Rest Life of Device + 2 years or life of	Third Party Mailing Agency Providers

	CET Numbers, NPI Numbers, Buying group data, marketing communications and responses, regional demographic data, IP Address				contract +2 years	
<b>Others Distributor Administration</b>	Address, Country, Email, Location data, Postal Code, Name, Phone number, IP Address		Direct Marketing, Administration, Customer relationship, Vendor Management:	Regulatory Auditors	Life of Device + 2 years or life of contract +2 years	Email
<b>End Customer Administration</b>	Address, Email, Country, IP Address, Location data, Name, Postal Code, Phone number, Photo	Health and Medical	Customer relationship, Administration, Compliance with law, Contract execution, Delivery Services, Vendor Management, Customer relationship, Administration, Compliance with law, Contract execution, Delivery Services, Vendor Management	Regulatory Auditors	Life of Device + 2 years or life of contract +2 years	Trade show leads, Sales Targets
<b>Others End Customer Data Capture</b>	Address, Country, Email, Location data, Postal Code, Name, Phone number, IP Address	Location Data	Direct Marketing	3 <sup>rd</sup> Party Marketing Provider	Life of Device + 2 years or life of contract +2 years	
<b>Others Clinical Retinal Images</b>	Photo Others: Could be personal information linked to image when provided	Biometric Data, Health and Medical, Vulnerable Persons (e.g. Children): It is possible to identify a young eye	Medical Research:	External Reading Centers	Minimum of 6 years after each subject signed an authorization	In House, From Medical Research and Practices



<b>Others Clinical Data for Medical Research</b>	Date Of Birth Initials	Biometric Data, Health and Medical, Racial / Ethnic origin, Vulnerable Persons (e.g. Children), Religious / Philosophical beliefs:	Medical Research:	Estenda External Grading by experts Third Party Service Providers	minimum of 6 years after each subject signed an authorization	In House, From Medical Research and Practices
<b>Applicant Administration - Recruitment - Offer Stage</b>	Identification Data, Profession and employment, Personal Characteristics, Education and Training	Religious / Philosophical beliefs	HR	Human Resource Service Agency	Perpetual for current employee, 7 years for post- employment.	
<b>Applicant Administration - Recruitment - Administration</b>	Personal Characteristics, Education and Training	Religious / Philosophical beliefs	HR	Human Resource Service Agency	2 Years	Human Resource Service Agency