

CONTENTS

Contents/Editorial Policy/
Nikon Group Profile

Message From the President

Sustainability Management

Creating Value

Environment

Society

Governance

Corporate Governance

Risk Management

Information Security and Cybersecurity

Thorough Compliance

Information Security and Cybersecurity

Basic Approach

At the Nikon Group, we believe that our information assets are the foundation of our corporate activities, and we treat information assets in accordance with the Nikon Group Information Security Policy. We have established several internal rules based on this policy and pursue information management that complies with the laws and regulations of each country and region. These rules and regulations are always available to employees via the corporate intranet portal. We continue to improve the level of operation through periodic education and compliance status checks.



▶ Nikon Group Information Security Policy

Strategy

Risk

Nikon may face operational disruptions and financial losses, including reduced revenue, in the event of a cyberattack that compromises our systems. Theft or leakage of confidential or personal information may also lead to reputational damage to our information management, resulting in a loss of trust in our company, and potential claims for damages.

Opportunities

Conducting proper information security measures and information asset management enables us to reduce our risk of cyberattacks. These measures help improve information availability, support business continuity, and enhance trust in the Nikon Group.

Strategy

The Nikon Group engages in systematic information security measures and information asset management to ensure business continuity and to enhance the trust of society. In the short-to-medium term, we intend to improve governance and cyber resilience incorporating zero-trust thinking, in addition to enhancing risk response and global security structure in connection with the use of AI. Over the long term, we will pursue preemptive risk management and the establishment of a security culture throughout the company. In this way, we aim to establish a company-wide risk management system that supports sustainable improvements in enterprise value.

Governance

The Nikon Group appoints the president as the head of information management, including personal information protection. We also established operating processes in accordance with Information Security Management Systems (ISMS*). The Information Security Department, under the supervision of the president, manages these operating processes and oversees them across the entire Group.

In addition, the heads of each organization of Nikon's business units, divisions, and Group companies are designated as information managers. By working with the Information Security Department, these individuals are establishing an information security management system compatible with the situation in each country and region, while comprehensively managing the entire Nikon Group.

The Information Security Department reports material matters involving information asset risks to the Information Security Meeting and the Risk Management and Compliance Committee (renamed in April 2025), which includes Executive Committee members. The department then translates the reported material matters into strategies and policies, and reports to the Information Security Meeting and the Risk Management Committee. The

department also sets measurable targets for these strategies and policies and tracks performance.

* ISMS: Information Security Management System

Healthcare Business Unit Initiatives

In the Healthcare Business, Nikon works to expand business in information services centered on digitalization, including support for network-based remote diagnosis and services that store and manage cloud-based pathology images. As business expands, we will be faced with handling more personal medical information for subjects and patients, which requires strict management at medical institutions. Given these circumstances, Nikon works to ensure thorough information security management. We not only increased the number of organizations subject to ISO 27001 in December 2023, but we also obtained ISO 27017 certification (a code of practice in information security management for cloud services) and launched operations.

Risk Management

The Nikon Group has created a security risk map that assesses the frequency and impact of risks. In connection with this map, we develop plans and implement response measures according to priority. We evaluate the effectiveness of these measures at the Information Security meetings, after which we incorporate the evaluation results in measures for the next fiscal year and beyond. In this way, we strengthen and improve the risk management process on an ongoing basis. Through these efforts, we identify risks systematically throughout the Group and improve security controls across the organization.

CONTENTS

Contents/Editorial Policy/
Nikon Group Profile

Message From the President

Sustainability Management

Creating Value

Environment

Society

Governance

Corporate Governance

Risk Management

Information Security and Cybersecurity

Thorough Compliance

Main Initiatives

Response to Information Security Incidents

The Nikon Group clearly defines information security incidents under the Nikon Group Information Management Rules. These regulations require the reporting of incidents from the department impacted to the Information Security Department. The Information Security Department works with relevant divisions to unify procedures from initial response to containment, impact assessment, and recovery, striving to minimize damage and impact, while resuming business operations promptly. Serious cases are promptly escalated to the responsible officer (CISO) for systematic decision-making and response.

In fiscal year 2025, we conducted an incident response drill with relevant divisions to confirm the effectiveness of our response procedures and communication system.

We have noted no serious information security incidents involving fines or compensation payments over the past three years.

Information Security Education

The Nikon Group conducts information security e-learning education programs as part of new employee training, etc., in order to raise employee awareness of information security and improve skills related to information security management. Beyond information management policies and rules, educational programs are designed to teach risk recognition and response methods based on actual case studies.

In addition, the Nikon Group Information Security Handbook, an educational document that provides easy-to-understand explanations of internal rules and the latest policies, is published on the portal site for all employees to refer to at any time. In this way, we make sure that every employee understands the importance of information asset management and complies with the rules based on a high level of awareness.

In fiscal year 2025, we started to roll out the information security education platform introduced to the Nikon Group in Japan in fiscal year 2024 to Group companies outside Japan, and began regular global e-learning education.

Information Security Audit

The Nikon Group periodically conducts internal audits pursuant to the Nikon Group Information Management Rules to confirm the appropriate implementation of information security measures.

In fiscal year 2025, we conducted written audits of all Group companies and divisions in Japan, as well as on-site audits of selected divisions based on key focus areas. We found no major nonconformities as a result of the audits.

In fiscal year 2026, we continue to conduct audits of key focus areas and verify the operational status of measures to ensure ongoing improvement throughout the Group.

Personal Information Protection

The Nikon Group has established the Nikon Group Privacy Protection Statement based on our respect for privacy and acknowledgment that processing personal data in a lawful and proper manner is an important social responsibility.

Additionally, under this statement, we established the Nikon Group Personal Data Processing Rules as a common set of rules covering the entire Group. We are now working to make these rules known within the Group and ensure that personal data is handled in accordance with these rules under the information management system. We conduct a questionnaire-based survey on the status of compliance with the Nikon Group Personal Data Processing Rules roughly once a year.

In addition, the Compliance Department oversees matters related to personal information and manages risk related to privacy and personal information for the entire Nikon Group.

Our specific initiatives include posting privacy notices on the website of each Nikon Group company in accordance with

relevant laws and regulations, and notifying customers of contact information for support regarding privacy and individual rights. This includes the purpose of use of personal information and how to delete their personal information.

In addition, we request that procurement partners follow the Nikon CSR Procurement Standards in order to maintain information security, including privacy protection.



- ▶ Nikon Group Privacy Protection Statement
- ▶ Privacy Notice of Nikon Europe B.V. in accordance with the EU General Data Protection Regulation (GDPR)
- ▶ Nikon CSR Procurement Standards

CONTENTS

Contents/Editorial Policy/
Nikon Group Profile

Message From the President

Sustainability Management

Creating Value

Environment

Society

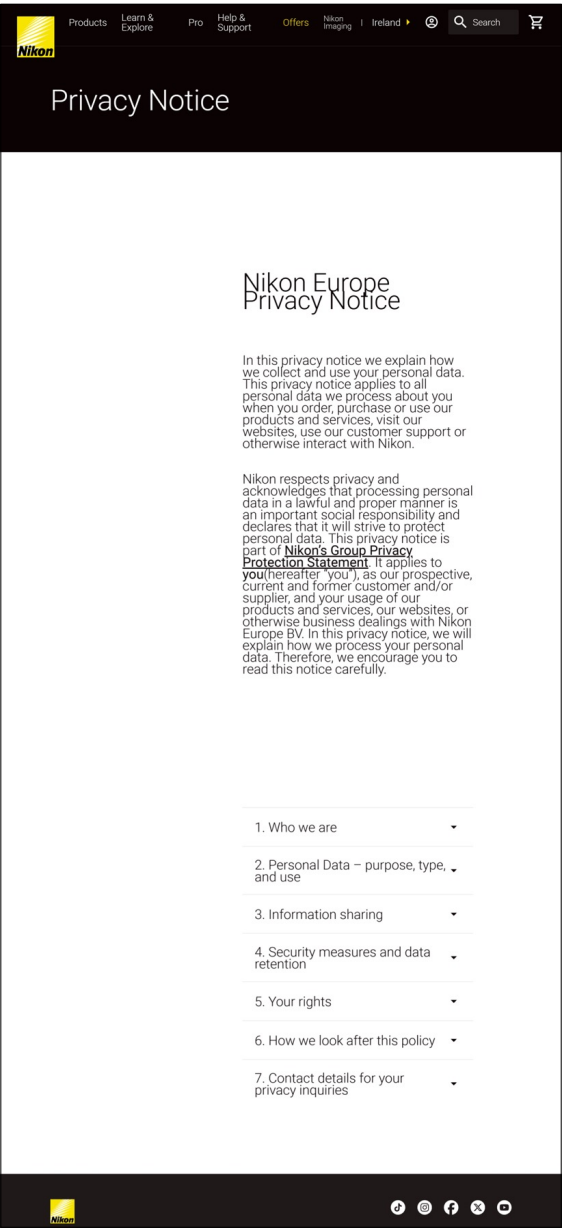
Governance

Corporate Governance

Risk Management

Information Security and Cybersecurity

Thorough Compliance



Privacy Notice of Nikon Europe B.V. in accordance with the EU General Data Protection Regulation (GDPR) (excerpt)

Response to the Personal Information Protection Laws of Each Country

The Nikon Group continuously monitors legislative developments related to personal data protection laws in each country and region, including the EU General Data Protection Regulation (GDPR), to ensure proper management of personal information under a robust information security system.

In fiscal year 2026, we will continue to take necessary actions in line with the enactment or revision of personal information protection-related laws and regulations in each country and region.

Improving Cybersecurity Infrastructure and Processes

The Nikon Group has established a comprehensive security system to improve cyber resilience to minimize the impact on business. Infrastructure protection promotes advanced governance through a combination of perimeter protection and zero-trust thinking. In addition, we visualize public assets at all locations as part of external surface threat management, and continuously monitor and correct misconfigurations in the cloud environment to prevent information leaks.

Furthermore, we continue to strengthen the process of ensuring safety from the early stages of development through detailed security by design in our products and services.