

## INFORMATION SECURITY AND DATA PROTECTION POLICY

EssilorLuxottica defines the Group policy on Information Security and Data Protection in compliance with European Union law and national law and guidelines issued by data protection Authorities, ISO/IEC 27001:2022, ISO/IEC 27701:2019, the HDS French regulation for cloud health data hosting and its Ethical Code. Information Security and Data Protection measures are implemented with additional health data management controls as defined in French regulation for HDS ensuring a stronger security approach in PII and Health Data Management. Therefore, the security process is in conformity with the principles of sustainable development ensuring the effectiveness, efficiency and quality of the internal processes and services provided to its clients.

A consistent application of the Code of Ethics is understood as an important element to ensure the confidentiality and the protection of the client's information, personal data, health data and other corporate assets. EssilorLuxottica has structured its Information Security Management System (ISMS) and Privacy Information Management System (PIMS), which is extended to HDS, to achieve the goals thereof. The Information Security and Privacy Management Systems are defined through risk analysis processes that are aimed at ensuring adherence to its Ethical Code, its service quality, safeguarding its own information, clients' information and interested parties' information.

EssilorLuxottica permanently works to ensure the protection of information according to data confidentiality, integrity, availability and prevents, in accordance with the best standards, unauthorised use, access, disclosure, amendment or deletion of data. It processes personal data in accordance with privacy principles and ensures that data subjects can assert their rights in accordance with relevant local laws.

EssilorLuxottica aims at having in place appropriate resources, including personnel, information, systems, and infrastructure to protect confidentiality, integrity and availability of information throughout the lifecycle of the data. To this end, it carries out specific controls over information security in compliance with applicable law and industry best practice.

Company's Top leadership ensures its commitment to the continuous improvement of its Information Security and Privacy Management, adherence to the law and its Ethical Code.

## MANAGEMENT DUTIES - OBJECTIVES

EssilorLuxottica has established and works to maintain the Information Security and Privacy Management Systems in compliance with ISO/IEC 27001:2022 and ISO/IEC27701:2019 and HDS certification requirements. Its objectives are outlined as follows:

- ✓ In accordance with the principles of confidentiality, integrity and availability, protection of the Company know-how, including its own information and clients' information, obtained, collected, received or produced throughout the projects and services carried out.
- ✓ Appropriate access limitation to ensure protection from unauthorised activity by EssilorLuxottica personnel, staff or by its general partners.
- ✓ Information security measures to protect its own and clients' information and personal data against breach, misuse, and fraud.
- ✓ Definition of both internal and external roles and responsibilities for information security and data protection.
- ✓ Provision of information security and data protection training and courses to EssilorLuxottica personnel and staff to increase knowledge about information security, privacy and risk minimisation.
- ✓ Continuity of information security and data in the event of a threat or adverse scenario.
- ✓ Compliance with the ISO/IEC 27001:2022 and ISO/IEC 27701:2019 standards and Référentiel de certification HDS.
- ✓ Adherence to contractual agreements, law and regulations on information security and data protection.

EssilorLuxottica management defines, disseminates, and maintains Information Security and Data Protection Policies at all levels within its organization:

- ✓ The Policies outline any change that may impact the Company's approach to information security and personal data management, including organizational changes, technical environment, availability of needed resources, legal, regulatory requirements, agreements, contractual obligations, reviews and audit outcomes.
- ✓ The Policies are kept up to date in compliance with applicable law, context and business requirements in accordance with the principles of continuous improvement of the Management System.
- ✓ The Policies track technological changes of information systems over time, including systems available to staff, central IT systems or cloud solutions.
- ✓ Privacy Policies are defined to conform with applicable law and contractual requirements. Where applicable, roles and responsibilities are outlined (whether EssilorLuxottica is the data controller and data processor, accordingly).

## **IMPLEMENTATION OF THE INTEGRATED ISMS and PIMS**

Company's Top leadership shares the principles and the objectives of the ISMS and PIMS and fully supports its implementation and maintenance.

Company's Top leadership approves the policy and ensures that the Company issues, communicates and makes it available to all interested parties as needed. The present information security policy constitutes a programmatic document of reference for all the other ISMS and PIMS documents.

The ISMS and PIMS include the policies and procedures implemented for the achievement of Information Security and Data Protection objectives. The ISMS and PIMS scope comprise all activities and processes needed to provide operational, administrative and support activities.

All employees, collaborators, providers, contractors, partners and third parties, that process EssilorLuxottica Group's information or EssilorLuxottica Group's client information, are required to adhere to the present information security and personal data protection policy. Managers in EssilorLuxottica are directly responsible for the policy implementation and adherence to it by the above parties.

EssilorLuxottica has drawn up, approved, published, and shared its policy and suitable internal documentation regarding Information Security and Data Protection with employees and interested parties.

The present policy is made available on the Company's official website. In accordance with the classification rules, relevant documents of the ISMS and PIMS may be shared with third parties and made available upon request.

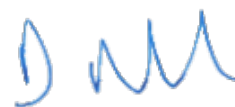
This policy is periodically reviewed and/or it is reviewed in the event of significant changes with possible impact on information security and personal data protection to ensure appropriateness, adequacy, effectiveness and adherence to law and standards.

27/09/2024



**Stefano Orsini**

**Group Risk, AP & Info Security  
EssilorLuxottica**



**Doris Marcellesi**

**Group Head of Compliance  
EssilorLuxottica**