WATCHES OF SWITZERLAND GROUP PLC

DATA PROTECTION AND INFORMATION SECURITY STATEMENT

THE WATCHES OF SWITZERLAND GROUP
DATA PROTECTION AND INFORMATION SECURITY STATEMENT

OUR COMMITMENT TO TRUST

This statement applies to all operations of Watches of Switzerland Group PLC across all territories where we conduct business. It is aimed at clients, partners, and stakeholders seeking assurance of our data protection and information security practices.

The Watches of Switzerland Group (the "Group") is a client-focused business committed to building lasting relationships through personalised experiences. To achieve this, we process personal data responsibly. While data is a valuable asset to the Group, it is even more vital to our clients' lives and identities. We recognise the trust placed in us and uphold it by protecting data and privacy in line with our Group values and Code of Ethics.

Data Protection and Information Security is not just a regulatory requirement, it underpins client confidence. Guided by our values, "We do the right thing. Always.", "We earn trust and confidence," and "We treat everyone with respect," we apply these principles to all personal data, whether relating to colleagues, clients, or others.

At WOSG, we treat personal information with the same care as our luxury products, safeguarding it through strong security, clear governance, and transparent practices to keep trust at the heart of everything we do.

THE WATCHES OF SWITZERLAND GROUP'S APPROACH TO DATA PROTECTION AND INFORMATION SECURITY

In the Group, data protection and information security go beyond compliance, they form a culture where every colleague understands their role in protecting client and business information. We aim to make this part of everyday behaviour, with shared responsibility for safeguarding personal data.

Our Group Policies apply to everyone, turning global obligations into clear commitments that guide daily actions. These underpin our training programme, supported by processes and role-specific detail. All colleagues complete data protection training at induction and annually.

Training is tailored to roles, ensuring colleagues understand responsibilities relevant to their functions. Awareness campaigns reinforce best practices throughout the year.

A GLOBAL APPROACH

The Group complies with all applicable laws and regulations in the countries where we operate. Our approach follows internationally recognised privacy and security principles, as reflected in the EU and UK GDPR, and sets minimum standards across all territories. We meet stricter local requirements where they apply and, where standards are lower, we adopt the higher standard for security, governance, fairness, and transparency, while using permitted

variations only where they do not harm clients or employees.

ACCOUNTABILITY, GOVERNANCE AND RISK MANAGEMENT

We maintain a structured horizon scanning process to identify and respond to emerging regulatory requirements and industry standards.

Data Protection and Information Security are critical business risks. Accountability lies with the Board via the Audit & Risk Committee, which receives regular reports from the Group Data Protection Officer (DPO) and Chief Technology Officer (CTO) on security maturity and compliance.

The IT and Data Steering Committee meets quarterly to assess risks and escalate issues. We maintain a Register of Processing Activities (ROPA) and strong processes for breach reporting, rights requests, and DPIAs/LIAs. DPIAs are mandatory for high-risk processing, with the DPO advising and monitoring.

We conduct regular risk assessments and data audits to ensure our approach remains proactive and responsive to evolving threats.

FAIRNESS, LAWFULNESS, TRANSPARENCY, AND RIGHTS

Our privacy policies and notices use clear, honest language. They meet regulatory requirements and explain why and how we process data, what we collect, who we share it with, retention periods, individuals' rights, and DPO contact details.

DATA SHARING

We share personal data with third parties only where a lawful basis exists and after confirming their ability to manage data securely. Contracts include provisions to protect data. For transfers outside the UK or EEA, we conduct risk assessments and apply approved legal mechanisms. Third-party relationships include contractual obligations for data protection and security.

SECURITY AND INFORMATION RESILIENCE

Personal data is stored securely using encrypted systems and controlled access. We apply retention schedules aligned with legal and business requirements.

We protect personal data through organisational and technical measures aligned with recognised standards, including NIST Cybersecurity Framework 2.0. Core controls include access management, encryption, secure development, vulnerability management, and regular testing. Privacy and cybersecurity by design are embedded across systems, with the Cyber team and DPO jointly assessing risks.

INCIDENT RESPONSE AND NOTIFICATIONS

We maintain procedures to detect, investigate and respond to personal data breaches. Where required by law, we will notify regulators and affected individuals without undue delay.

THIRD-PARTY ASSURANCE

As a curator of some of the world's leading luxury brands, we work with a global network of brand partners. We hold these brand partners to the same high standards we set for ourselves. We conduct due diligence to ensure information remains protected throughout the supply chain.

ETHICS AND INTEGRITY; WHISTLEBLOWING

We aim to conduct our business with the highest standards of honesty and integrity and encourage colleagues to raise any concerns about the way we use or protect personal data. The Company has developed a Code of Ethics and a Whistleblowing policy both of which can be found on the corporate website www.thewosgroupplc.com.

If a colleague suspects that the principles of data protection or the internal Policy are not being followed, personal data is being put at risk, or if something just does not feel right, they can speak, in

confidence, to the DPO. Colleagues are also made aware of this in an internal policy and annual data protection training. Colleagues can also speak to their Line Manager or the Executive Director, Human Resources.

If it is not possible to raise concerns through these channels the Company provides an independent and external facility managed by Safecall. Reporting details can be found in the Whistleblowing Policy.

CONTACT

For data protection queries, contact DPO@thewosgroup.com. For cyber security matters, email Cybersecurity@thewosgroup.com.

The Company will take steps to monitor compliance with this Policy.

Approved by the Watches of Switzerland Group PLC Board on 26 February 2026.