THE WATCHES OF SWITZERLAND GROUP

WATCHES OF SWITZERLAND GROUP PLC

DATA PROTECTION AND INFORMATION SECURITY STATEMENT

WATCHES OF SWITZERLAND GROUP
DATA PROTECTION AND INFORMATION SECURITY STATEMENT

The Watches of Switzerland Group is an international retailer of world leading luxury watch brands with a growing complement of luxury jewellery brands. The Group provides clients with the finest selection of luxury timepieces from all of the major groups and independent brands together with an impressive presentation of smaller independent brands. Our Group comprises Watches of Switzerland, Goldsmiths, Mappin & Webb, Mayors, Betteridge, Analogue Shift, our mono brand boutiques and any brands or companies that may become part of our business. You can find more detailed information about the Group on our corporate website www.thewosgroupplc.com.

As a client-centred business that looks to build strong and lasting relationships with its clients and provide a personalised experience, we need to process personal data. While that data is an important asset to the Watches of Switzerland Group ('WOSG,' 'Group,' or 'our group'), more importantly it is vital to the lives and identities of our clients. We understand the trust clients place in us and seek to repay it in the way we use and protect their data and privacy, in line with our company values. Of those values, the following are particularly pertinent to data protection: 'We do the right thing. Always.,' 'We earn trust and confidence,' and 'We treat everyone with respect' and with our Code of Ethics. This applies equally to personal data about past, present, and prospective employees, and any other people whose data we may use.

The WOSG approach to data protection

Data protection is more than a matter of legal compliance. We aim to create an internal culture where all colleagues understand the importance of data protection both to clients, fellow colleagues, and business, and make it part of their everyday behaviour, and which encourages shared accountability for safeguarding personal data.

WOSG's internal Data Protection Policy underpins this. It applies to all who work in or for the Group anywhere, in any role, and is designed to be simple and understandable to encourage engagement and compliance. It distils our global data protection obligations into a set of clear, universally applicable high-level commitments to guide day to day behaviour. These in turn form the backbone of our internal training which, along with applicable processes, procedures, and other internal policies, sets those commitments in context and gives the role-, function- or location-specific detail needed to apply them in practice. We require all colleagues to complete the data protection training at induction and annually thereafter.

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 Whistleblowing policy which can be found on the corporate website.

If a colleague suspects that the principles of data protection or the Data Protection Policy are not being followed, personal data is being put at risk, or if something just does not feel right, they can arrange to speak in confidence to the Group's Data Protection Officer. They are made aware of this in the internal Data Protection Policy and e-Learning and reminded periodically. They 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.

A Global Approach

WOSG must comply with applicable law and regulation in the countries in which it operates. Our overall approach is based around internationally accepted privacy principles as embodied and enhanced in the EU and UK General Data Protection Regulation ('GDPR') and sets out the minimum standards we will apply in the territories within which we operate. We will comply with local data protection requirements where they are stricter. Where standards are lower or less prescriptive, we will always seek to apply the higher standard on matters of security, governance, fairness, and transparency while taking advantage of permitted variations on matters such as marketing or regulatory reporting. Where there is any apparent conflict between WOSG policy or business procedure and local data protection law, the Group's Data Protection Officer (DPO) will guide the business in finding an acceptable solution. The Data Protection Officer can be contacted at DPO@thewosgroup.com.

Accountability, Governance and Risk Management

The Group has appointed a data protection officer, who is responsible for all matters relating to data protection and advises and guides the Group in achieving compliance with its obligations and managing data protection risks. The DPO is independent and works closely with key business areas to encourage a 'Privacy by Design and by Default' approach, and to ensure the Group's overall strategy for using and maintaining its data aligns with data protection requirements and policy.

The Group has established a Data and Cyber Steering Group which meets quarterly to take formal decisions and assess risks on matters relating to data protection and data security, escalating issues and risks to the Audit & Risk Committee where appropriate.

The Group maintains a register of its data processing activities (often known as a 'ROPA'), which is updated annually or when necessary, and processes for reporting and handling data breaches and responding to data rights requests. We conduct Data Protection Impact Assessments and Legitimate Interests Assessments where appropriate. The Internal Audit and Stores Audit Teams monitor policy compliance, and the Group may commission or conduct additional reviews or audits as required.

Fairness, Lawfulness, Transparency, and rights

WOSG has a clear legal basis for all the personal data it collects. Our client - and colleague - facing privacy policies, notices and consent wordings are clear, honest, and designed to be understandable, and we take steps to ensure data minimisation and purpose limitation. We have straightforward processes by which people can withdraw consent where applicable and seek to exercise their other data rights, such as subject access, objection, rectification, and erasure. DPO contact details are given on our public-facing and internal data policies and privacy notices.

Data management

The Group has a Head of Business Intelligence Analytics and Data Governance, who is responsible for the Group's strategy for using and maintaining its data, and we take steps to maintain the accuracy, integrity and quality of that data and ensure we do not hold it any longer than necessary for the purpose for which we first collected it.

Data sharing

WOSG shares data with third parties only where it has a valid legal basis for doing so. We conduct due diligence on brand partners and other suppliers to ensure that they can and will handle our data securely and appropriately, and we include the relevant legal provisions in our contracts. When transferring data from the UK or Europe to the US or other 'third countries' not deemed to offer the same level of protection as GDPR/UK GDPR, we complete the required Transfer Risk Assessments and use permitted legal transfer mechanisms.

WOSG does not sell client data.

Security

We safeguard personal data against loss, damage, destruction, unauthorised use/access, or disclosure using both technical and non-technical ('organisational') means. Examples of non-technical measures we use are mandatory data protection and security training for colleagues, system and building access controls, and due diligence checks on brand partners and suppliers.

The Group has a dedicated cyber security team which ensures that a range of technical security measures and controls is in place around personal data and the systems, networks, and equipment on which we process it. We review these controls continuously to ensure they remain appropriate to known and emerging threats. They include data loss prevention and alerting tools, anti-malware and virus protection, and threat/intrusion detection tools. We conduct regular penetration testing on key systems. The Cyber team works closely with the Group's DPO to create and maintain a robust, joined-up data protection and security framework and guide the business in managing risks effectively.

Contact

For further information about data protection within WOSG, contact the DPO at DPO@thewosgroup.com. For more information about Cyber Security, please contact the Group's Cyber Manager at Cybersecurity@thewosgroup.com.

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

Approved by the Watches of Switzerland Group PLC Board on 28 February 2024.