CCTV Policy

Document Control Information			
Version	1.0	Author	GDPRLocal
Reviewer		Review Date	
Review Frequency	12 months	Next Review Date	August, 2025

The current version of this document is up to date. Any future versions or changes to this document must also be approved by the author and the Executive Team and issued on a version-controlled basis under their signature. This document has been stored at Safe Storage.

Aim

The Aim of this CCTV Policy is to outline the policies and practices regarding the use of CCTV within our premises. Its primary aim is to provide clear information about the purposes, scope, and management of surveillance measures, ensuring transparency and compliance with applicable data protection laws. By detailing how and why these technologies are employed, we aim to safeguard individuals' privacy, maintain security, and uphold the highest standards of ethical conduct in our operations.

Intro

In line with data protection laws, including the General Data Protection Regulation (GDPR), this document outlines our practices for the use of CCTV technology. It details how these surveillance measures are implemented, the purposes they serve, and the measures in place to ensure they are used responsibly. Additionally, this document provides information about the rights of data subjects, ensuring they are aware of how their personal data is handled and what rights they have under the applicable data protection laws. This introduction aims to provide transparency regarding our surveillance practices and to inform all relevant parties about our commitment to protecting personal data and upholding legal standards.

Definitions

The General Data Protection Regulations/GDPR - Whenever the terms 'The General Data Protection Regulations' or GDPR' are referred to in this document, it usually pertains to both The Regulation (EU) 2016/679 (EU GDPR) and The Data Protection Act 2018 (UK GDPR). Should there be a need to invoke other regulations, they will be appropriately and distinctly named.

The Regulation (EU) 2016/679 (EU GDPR) Territorial scope - The territorial scope of the GDPR encompasses the processing of personal data by entities established within the European Union, regardless of where the processing occurs, as well as entities outside the EU that either offer goods or services to individuals within the EU or monitor their behaviour within the Union. It also applies in situations governed by a Member State's public international law. This means the GDPR's reach extends beyond the EU's borders, affecting organizations globally that interact with EU residents.

The Data Protection Act 2018 (UK GDPR) Territorial Scope - The UK GDPR, which came into effect post-Brexit, maintains similar territorial principles. It applies to the processing of personal data by entities established within the United Kingdom. For entities outside the UK, the UK GDPR applies if they offer goods or services to, or monitor the behaviour of, individuals within the UK. It also captures situations dictated by UK international law.

Personal data [personal data] - 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Type of Data - Under the General Data Protection Regulation (GDPR), 'sensitive data' is defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Processing - Any operation or set of operations performed on personal data, whether or not by automated means. This includes collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.

Third-Party/Vendor - A natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

The Purpose of Processing Personal Data

Gym Spa Soho Lt. implements CCTV technology to enhance the safety and security of our facilities. The primary purposes for processing personal data through these systems are as follows:

1. **Security and Safety:** To protect our clients, employees, and premises from physical harm or abusive behaviour. Surveillance helps us identify individuals who have previously engaged in violent or disruptive conduct, enabling us to prevent such individuals from re-entering our facilities.
2. **Incident Prevention and Response:** To deter and address incidents of physical abuse or other security threats effectively. By monitoring and reviewing footage, we can respond promptly to any suspicious or harmful behaviour, ensuring a safe environment for everyone.
3. **Access Control:** To manage and restrict access based on historical behaviour. Individuals identified as having previously engaged in abusive actions can be barred from entering our premises, thereby reducing the risk of future incidents.
4. **Compliance and Evidence:** To provide evidence in the event of security incidents or disputes, ensuring that we can support investigations and comply with legal requirements effectively.

The use of CCTV technology is conducted with the utmost respect for privacy and in accordance with relevant data protection laws. We ensure that personal data is processed fairly, transparently, and securely.

Categories of Data That Are Processed

In the course of operating our CCTV systems, Gym Spa Soho Ltd. processes the following categories of personal data:

- **Visual Images:** CCTV footage includes recorded images and video of individuals as captured by our surveillance cameras. This encompasses general footage of clients, members, employees, contractors, and other persons entering or within the premises.
- **Audio Data:** CCTV systems equipped with microphones also capture recorded audio, including conversations and ambient sounds within the camera's range.
- **Incident Data:** Data related to security incidents, including details of individuals involved, their actions, and the outcomes of any investigations.

This data is processed solely for the purposes outlined in this policy and is handled with strict confidentiality and security measures. Access to this data is restricted to senior management only, and we take all necessary steps to ensure compliance with data protection regulations.

Who is Responsible for the Processing of Personal Data

The responsibility for the processing of personal data through our CCTV systems lies with Gym Spa Soho Ltd. As the data controller, Gym Spa Soho Ltd. ensures that all processing activities comply with applicable data protection regulations.

Senior management within Gym Spa Soho Ltd. is the only group authorised to conduct video surveillance and make decisions based on the data collected. This responsibility includes overseeing the operation of CCTV systems, reviewing recorded footage, and taking actions based on the analysis of this data. Additionally, senior management is tasked with ensuring that all processing activities are carried out in accordance with data protection laws and company policies. This involves implementing appropriate security measures, handling data requests, and maintaining transparency with data subjects.

By designating senior management as the responsible personnel, we aim to ensure that our surveillance practices are conducted with the highest level of oversight and adherence to legal and ethical standards.

Lawful Basis of Processing of Personal Data

The processing of personal data through our CCTV is conducted under the lawful basis of Legitimate Interest, as outlined in the General Data Protection Regulation (GDPR).

Our use of these technologies is grounded in the necessity to enhance the security and safety of our clients, employees, and premises. The legitimate interests we pursue include:

- **Enhancing Security:** Implementing surveillance to protect against physical abuse and security threats, ensuring a safe environment within our facilities.
- **Preventing Abuse:** Identifying and barring individuals who have previously engaged in abusive behaviour to prevent future incidents and maintain a secure space for all users.
- **Investigating Incidents:** Using recorded footage to investigate security incidents and ensure a prompt and effective response to any threats or disruptive behaviour.

We have conducted a Legitimate Interest Assessment (LIA) to evaluate and confirm that our legitimate interests in processing personal data through CCTV do not override the rights and freedoms of the individuals captured. This assessment ensures that our processing activities are balanced, necessary, and proportionate, aligning with our security objectives while adhering to data protection principles.

Who Has Access to the Personal Data Collected

Access to the personal data collected through our CCTV systems is restricted to ensure confidentiality and security. Senior management within Gym Spa Soho Ltd. is the primary group authorised to access personal data. They oversee the operation of the surveillance systems, review recorded footage, and make decisions based on the data collected. This access is strictly controlled to ensure it is used solely for the purposes outlined in this policy.

In the event of a formal investigation, such as by law enforcement, police authorities may also have access to the data as required by the investigation. This access is granted in accordance with legal procedures and is subject to appropriate safeguards to protect data privacy.

Additionally, an IT Administrator may have access to the data solely for maintenance purposes. The IT Administrator's access is limited to performing necessary technical support and ensuring the proper functioning of the systems, without involvement in the review or decision-making processes related to the data.

Access to personal data is governed by strict protocols and security measures to prevent unauthorised use or disclosure. All individuals with access are required to adhere to our privacy policies and procedures.

Rights of Data Subjects

As part of our commitment to data protection and privacy, we ensure that individuals have clear rights regarding their personal data collected through CCTV. Under the General Data Protection Regulation (GDPR) and applicable data protection laws, data subjects have the following rights:

1. **Right to be Informed** Data subjects have the right to be informed about the collection and processing of their personal data. This policy serves to provide transparent information about the purposes and scope of CCTV technology implemented at our premises.
2. **Right of Access** Data subjects have the right to request access to their personal data held by us. This includes obtaining a copy of their data captured by CCTV systems. Requests for access can be made to the Data Protection Lead (DPL).
3. **Right to Rectification** If personal data held about an individual is inaccurate or incomplete, data subjects have the right to request that it be corrected or completed. This ensures that the data we hold is accurate and up-to-date.
4. **Right to Erasure** Under certain circumstances, data subjects may request the erasure of their personal data. This right is subject to conditions where data may need to be retained for legal or legitimate purposes, such as compliance with legal obligations or for the establishment, exercise, or defence of legal claims.
5. **Right to Restriction of Processing** Data subjects have the right to request the restriction of processing their personal data under specific conditions. During such a period, data processing will be limited, and the data will not be used except for storage purposes or with the data subject's consent.
6. **Right to Data Portability** Where applicable, data subjects have the right to request that their personal data be transferred to another data controller in a structured, commonly used, and machine-readable format. This right is generally applicable to data provided by the data subject and processed by automated means.
7. **Right to Object** Data subjects have the right to object to the processing of their personal data based on legitimate interests. If a data subject objects to processing based on legitimate interests, we must demonstrate compelling legitimate grounds for continuing the processing.
8. **Right Not to be Subject to Automated Decision-Making** Data subjects have the right to not be subject to decisions based solely on automated processing, including profiling, which significantly affects them. This right ensures that individuals are not unfairly impacted by decisions made without human intervention.
9. **Right to Complain** Data subjects have the right to lodge a complaint with a supervisory authority if they believe that their rights have been infringed. In the UK, this is typically the Information Commissioner's Office (ICO), and in the EU, it is the relevant data protection

authority in the member state where the individual resides.

Exercise of Rights

To exercise any of the above rights, data subjects should contact the Data Protection Lead (DPL) at Gym Spa Soho Ltd. We will acknowledge and respond to any requests in accordance with legal requirements and within the prescribed timeframes. The contact information of our DLP are as follows:

Name of Data Protection Lead: Dan Hazlewood
Company name: Gym Spa Soho Ltd.
Data Protection Lead Address: Ramillies House, 1-2 Ramillies st. Soho London W1F 7LN
Data Protection Lead Number: 0204 519 6044

For more information regarding our practices if a request by a data subject is submitted to us, please refer to our Subject Access Request Policy.

When Will the Processing Begin

The processing of personal data through CCTV systems will begin as soon as a data subject enters the premises. This includes the capture and analysis of visual, audio, and biometric data upon entry.

Security of the Personal Data

To ensure the security and integrity of both CCTV data, we implement strong technical and organisational measures to protect against unauthorised processing, accidental loss, destruction, or damage.

1. **Data Security Measures:** CCTV data are encrypted and initially stored locally. Backups are created on a secure server and transferred to a USB drive if needed for police use. The server operates on a secure LAN with Windows Server 2022 and encrypted disks, with access restricted to senior management.
2. **Protection Against Unauthorised Processing:** Access to both CCTV systems is controlled through secure authentication methods and strong password protocols, guided by our Access Control and Password Policy.
3. **Measures for Processors:** When engaging third-party processors for storing or managing CCTV data, we ensure compliance through strict contractual agreements that include data protection clauses. Regular audits are conducted to ensure ongoing adherence to security measures and data protection laws.
4. **Safeguarding International Transfers:** Currently, we do not transfer CCTV data internationally. Should such transfers become necessary, we will implement appropriate safeguards such as Data Protection Addendums (DPAs) and Standard Contractual Clauses (SCCs) to ensure compliance with international data protection requirements.

Retention Period

Personal data captured through CCTV will be retained for a period of 90 days from the date of its initial capture. After this period, the data will be securely deleted or anonymised in accordance with our data retention and deletion policies.

If you wish to learn more about our data retention practices please refer to our Data Retention Policy.

Governance of this document

Our organization views data protection as a critical component of our overall security and privacy strategy. This policy is overseen and owned by our Data Protection Lead (DPL). This key document emphasizes the paramount importance of data in the digital era, mandating a review and update every 12 months by the DPL to ensure continued relevance and compliance. Breaches or non-compliance should be promptly reported to the DPL, highlighting our steadfast commitment to safeguarding our stakeholders' interests.

End.