

Data Protection Impact Assessment (DPIA)

Project: Outsourced Control Room - CCTV & Guard Monitoring

Location of Processing: South Africa

Date: 30th July 2025

Version: 1.1

Completed by: Neil Jones – Managing Director

1. Purpose of the Processing

SmartWatch Solutions Ltd has outsourced live CCTV monitoring and security guard activity monitoring to a South Africa based control room. The control room is exclusively responsible for overseeing SmartWatch sites only.

Its responsibilities include:

- Live CCTV monitoring and incident response
- Guard booking on/off sites using Timegate
- Hourly welfare check calls to deployed guards

Nature of data processed:

- Live CCTV footage (may capture identifiable individuals)
- Audio (e.g. body-worn cameras, intercoms)
- Alarm events and recorded footage
- Staff names, shift patterns, and attendance logs
- Call records and monitoring activity logs
- Operator generated logs and reports

Type of individuals involved:

- Members of the public
- Site workers
- Security personnel (SmartWatch employed guards & labour providers)
- Visitors to monitored sites

2. Lawful Basis for Processing

Lawful basis under UK GDPR:

- Article 6(1)(f) – Legitimate Interests: The processing is necessary to protect sites, staff, and individuals against crime, unauthorised access, and welfare risks.

- Article 6(1)(b) – Necessary for performance of a contract (employee monitoring for operational delivery)
- Where applicable:
 - Article 9(2)(g) – Substantial public interest for processing special category data (e.g. criminal activity).

3. Description of Processing

How is data collected?

- CCTV cameras and NVRs installed on UK based customer sites
- SmartWatch's guard management system (Timegate)
- Voice and alarm signals received by operators

How is data accessed or viewed?

- Via secure, web-based platforms (Immix for CCTV and Timegate for guard monitoring)
- Platforms are hosted in the UK and accessed remotely via secure VPN by authorised control room staff

How is data stored and deleted?

- CCTV footage stored on local site NVRs, subject to automatic deletion (e.g. after 30 days)
- Timegate data stored in UK data centres managed by SmartWatch
- Exported logs or footage are time-limited and securely deleted after investigation resolution

Who has access?

- Authorised South African control room operators
- SmartWatch management and system administrators in the UK
- Authorised customer representatives (with role-based access)

4. International Data Transfers

Is personal data transferred or accessed outside the UK?

Yes – accessed in South Africa for monitoring SmartWatch operations

Safeguards in place:

- A UK approved International Data Transfer Agreement (IDTA) is in place
- Web platforms (Immix and Timegate) are hosted in the UK with admin control by SmartWatch
- South African control room only monitors SmartWatch sites and users
- Access is via secure VPN
- Data access is logged and auditable by UK administrators
- Staff are trained in GDPR and follow contractual obligations

5. Risks to Individuals

Risk	Likelihood	Impact	Mitigation
Unauthorised access to CCTV or staff data	Medium	High	VPN with MFA access control, audit trail
Misuse of personal or shift data by operators	Low	Medium	Contracts, training, UK admin monitoring
Inaccurate guard attendance or call logs	Medium	Medium	Automated logging, supervisor validation
Breach of footage or call recordings	Low	High	Time limited access, encryption, UK oversight

6. Measures to Reduce Risk

- End-to-end encryption on all video streams and login sessions
- Secure VPN access with MFA for all remote connections
- SmartWatch retains administrator control over Immix and Timegate
- Full audit trails for user access and activity
- Operator training, vetting, and role based access
- Regular reviews of DPA, IDTA, and access logs
- UK based oversight of monitoring activities and incident escalations

7. Consultation

Have data subjects been consulted?

Yes

No – not required (processing is proportionate, signage and policy coverage provided)

Has internal legal / DPO / IT been consulted?

Yes – We have consulted with our IT security provider, BCN.

Has the overseas partner completed a security questionnaire or provided their policies?

Yes – Attached as Appendix A

No – Awaiting response


8. Outcome of DPIA

- Proceed with processing
- Proceed with changes
- Do not proceed

9. Review Schedule

DPIA to be reviewed annually or upon material change to systems, suppliers or processing scope.

10. Sign-Off

Name	Role	Signature	Date
Neil Jones	Managing Director		30 th July 2025