Legitimate Interest Assessment

Customer/Project Code	Securys Ltd	
Reference	N/A	
Process Name	CCTV recording	
Regulatory Jurisdiction(s)	United Kingdom	
Data Controller	Securys Ltd	
Data Protection Officer		where applicable
Data Controller contact(s)	Securys Ltd 161-165 Farringdon Road London EC1R 3AL email: privacy@securys.co.uk telephone: 0800 193 8700	
Data Processor(s)	Microsoft Corporation	where applicable
Data Processor contact(s)	N/A	
Assessment conducted by	Bart van der Geest	
Document date	08/01/2020	
Document status	DRAFT	
Document version	v1.0	

Findings

Summary of Controller's Legitimate Interests	**Summary of Impact on Data Subjects**	**Commentary on Balancing Test**
Securys has a legitimate interest in deterring and detecting crime.	Data subjects affected by the processing may experience increased stress and anxiety due to their privacy being invaded. In case of a data breach, data subjects may experience increased levels of anxiety and a loss of control of their personal data.	To minimise the impact of the processing on data subjects, Securys has taken appropriate measures to ensure that CCTV footage is encrypted, that access to the footage is limited, and that footage is retained for no longer than 31 days, unless the footage is specifically selected for retention. We believe that in implementing these measures, a fair balance is achieved between the rights of individuals and Securys' legitimate interest.

Can the data controller rely on legitimate interest as the lawful basis for the proposed processing?	**Yes**

Assessment reviewed by	Ben Rapp	
Role	Principal	
Date	21/01/2020	
Assessment approved?		**Yes**

Comments

Next Review Date	

References

Privacy policies	CCTV Privacy Notice (https://www.securys.co.uk/cctv)
Data subject rights policies	
Data sharing agreements	
Records of data processing	
Other supporting materials	

Template ©2020 Securys Limited	
Template version	1.1
Template date	02 January 2020
Last changed by	JL
Last change	reformatted to fit Excel template

Overview

Summarise the processing in context	This processing involves video recording by a closed-circuit television (CCTV) system. The CCTV system covers the third floor of the building including the stairwell lobbies as well as the interior of Securys' office. The system does not capture sound or use automated facial recognition capabilities. The CCTV recordings are collected by Securys, and stored locally on a discrete device. CCTV footage is encrypted and retained in the database for 31 days after which they are automatically deleted unless specifically selected for retention. CCTV recordings are only inspected or processed beyond collection where this is deemed necessary as part of an investigation into a suspected incident. In limited circumstances, Securys may inspect recordings for routine testing purposes, but will ensure to use footage containing only staff members who have previously been notified of the test and given the option to opt-out.
Why is a Legitimate Interest Assessment required?	A Legitimate Interest Assessment is required as the processing is carried out on the basis of Article 6(1)(f) GDPR - legitimate interest.
Does this processing require a Data Protection Impact Assessment?	Yes
If yes, give details of the completion and result of the Data Protection Impact Assessment.	A Data Protection Impact Assessment (DPIA) was completed to assess the process and to see if the process was likely to result in a high risk to the rights and freedoms of individuals. The DPIA concluded that a proportionate balance had been struck between the rights and freedoms of individuals and Securys' legitimate interest, and that the processing was not likely to result in a high risk.
Will individuals be able to opt out of this processing?	No
If no, explain why not and how data subjects' rights will be respected.	Individuals are unable to opt-out of collection as the CCTV system is permanently in operation, and any limitation to the processing would compromise Securys' ability to use the CCTV system for its intended use. Data subjects will still be able to exercise their data subject rights, including the right to receive a copy of their data and the right to erasure.

Data Processing

Describe the data subjects involved in processing.	The data subjects involved in the processing include employees, candidates, contractors, suppliers and visitors.
Describe the categories of data involved in processing.	The categories of data processed include physical characteristics, behavioural data and location data.

Does the processing include any of the following categories of data?

racial or ethinic origin	No	
religion and/or philosophical beliefs	No	
trades union membership	No	
genetic data	No	
biometric data for the purpose of uniquely idenitfying a person	No	
health	No	
sexual orientation	No	
sex life	No	
criminal convictions and offences	No	

Is there any data which people are likely to consider particularly 'private'?	No	
Is there processing of children's data?	No	
Is there processing of data relating to vulnerable adults?	No	
Does the data relate to people in their personal or professional capacity?	The data processed relates to people in their personal and professional capacity.	

Describe the technology used in processing, including novelty and prior concerns.	Self-contained 4-camera wireless IP CCTV system with recording.

Purpose

Why is the data being processed?	The data is processed for the purpose of deterring and detecting crime. In rare instances, the recordings may also be used by Securys to defend against a legal claim.	
What benefit does the data controller/processor expect to gain from the processing?	Benefits from the processing include the detection and prevention of criminal activity and behaviour, increased security, and the protection of Securys' resources.	
Do any third parties benefit from the processing?	No	
Are there any wider public benefits to the processing?	No wider public benefits are involved in this process.	
How important are the benefits that have been identified?	The benefits are important for security purposes, as well as to protect Securys' business integrity and reputation.	
What would be the impact if the data could not be processed as proposed?	Restriction of the proposed processing would significantly limit Securys' ability to deter and detect crime.	
Does the processing require compliance with any specific data protection rules (e.g. profiling requirements, or e-privacy legislation)?	Yes	The processing requires compliance with the General Data Protection Regulation and the UK Data Protection Act 2018.
Does the processing comply with other relevant laws?	No	
Does the processing comply with industry guidelines or codes of practice?	Yes	The processing complies with the ICO's code of practice for surveillance cameras and personal information.
Are there any other ethical issues with the processing?	No	

Necessity

How will this processing help the data controller to achieve the stated purpose?	Video footage from the CCTV system will help identify criminal activity and behaviour, and gather evidence required for the investigation of a crime. The presence of CCTV cameras could also help deter individuals from committing a crime.	
Is the processing proportionate to that purpose?	Yes	
Can the same purpose be achieved without the proposed processing?	No	The purposes could not be achieved without the proposed processing.
Can the same purpose be achieved by processing less data, or by processing the data in another more obvious or less intrusive way?	No	The purposes could not be achieved by processing less data, given that this would compromise the effectiveness of the CCTV system. Other possible preventitive methods were explored, however, we concluded that these methods were less effective for the purpose of detecting and deterring crime.

Reasonable Expectations

Does the processor have an existing relationship with the individual?	Yes	
What is the nature of the relationship and how has the processor used data in the past?	Individuals affected by the processing are: 1. Securys employees and candidates; 2. Have a business relationship with Securys. 3. Have a personal relationship with a Securys employee. 4. Have a business relationship with the Securys Principal outside the normal course of Securys's business.	
Was the data collected directly from the individual? What did the processor tell them at the time?	Yes	Individuals are informed of the CCTV recording by the CCTV notice displayed outside the office. Alternatively, individuals are made aware of the CCTV recording if they read the CCTV Privacy Policy on Securys' website. Securys employees were informed prior to the commencement of the processing.
If the data was obtained from a third party (including for another purpose), what did the third party tell the individuals about reuse (for other purposes)? Does this adequately cover this process and processor?	N/A	
How long ago was the data collected? Are there any changes in technology or context since then that would affect expectations?	This is a new process.	
Is the data contorller's/processor's intended purpose and method widely understood?	Securys believes that the purpose for processing is widely understood.	
Is the data controller/processor intending to do anything which might be considered new or innovative?	No	
Is there any evidence about data subjects' expectations with regard to the processing? (e.g. from market research, focus groups or other forms of consultation)	No	
Are there any other factors in the particular circumstances that mean the data subject would or would not expect the processing?	Data subjects could reasonably expect CCTV recording to take place at Securys' office.	

Likely Impact

What are the possible impacts of the processing on individuals?	Data subjects affected by the processing may experience increased stress and anxiety due to their privacy being invaded. If Securys' CCTV recordings were breached, data subjects could experience increased levels of anxiety, and a lack of control of their personal data. A data breach may also create a lack of trust in Securys and damage our reputation.	
Will individuals lose any control over the use of their personal data?	Yes	In some circumstances, subject access requests may be rejected if they are deemed to be unreasonable, would compromise an investigation into a suspected incident, or infringe upon the rights and freedoms of other data subjects.
What is the likelihood and severity of any potential impact?		The likelihood of any potential impact is low due to CCTV recordings being encrypted and Securys' compliance with the ISO 27001:2013 information security standard.
Are some people likely to object to the processing or find it intrusive?	Yes	There is a possibility that data subjects would object to the processing or find it intrusive.
Would you be happy to explain the processing to individuals?	Yes	Securys is prepared to explain the processing to individuals where such a request is reasonable.
Can Securys adopt any safeguards to minimise the impact?	Yes	In order to minimise any potential impact, Securys has employed encryption, implemented access controls and adopted a retention period.