Closed Circuit Television Policy

General Data Protection Regulations

GDPR 2016 / 679 – 2018

Data Protection Acts 1988, 2003 & 2018

Issue No.	Reviewed By	Approved By	Approval Date	Details of Change	Originator
Issue 01	Management	Westdoc		Comments / amendments agreed	Matt Breslin

Author:	Westdoc Data Protection Officer General Data Protection Regulations GDPR 2016 / 679 - 2018 Data Protection Act - 2018
Creation Date:	01.07.2020
Review Date:	01.07.2021
Related Policies:	Data Protection Policy Data Breach Policy Data Access Request Policy Document Retention Policy Privacy Impact Statement Data Protection Impact Statement Data Breach Management Policy Staff Privacy Notice

Table of Contents

1 INTRODUCTION

Westdoc Closed Circuit Television Policy CCTV provides guidance and clarity to all those impacted either directly or indirectly by the use of CCTV footage in the Organisation.

2 PURPOSE

Westdoc as a Data Controller and Processor is fully committed to providing guidance, information and transparency pertaining to its use of CCTV footage across the Organisation.

3 SCOPE

Westdoc's CCTV footage Policy extends to the entire organisation.

4 DEFINITIONS

A Data Controller is defined as any person / entity who, whether alone or with others controls the purposes and means of processing of Personal Data as outlined under Article 4 of the General Data Protection Regulations GDPR 2018.

Personal Data:

Personal Data is defined in Article 4 (1) of the GDPR Regulations, it refers to any information relating to an identified or identifiable natural person. The Data Subject who can be identified, directly or indirectly. In particular, by reference to an identifier such as a name, number, location, DOB or to one or more factors specific to the physical, generic economic or social identify of that natural person.

Data Subject: is a living individual, the subject matter of the Personal Data. It should be noted that the GDPR Regulations do not apply to deceased persons and to their data.

Data Processing:

Data Processing has a wide definition and scope and it includes the following processes. It means performing an operation or series of operations. It covers collection, recording, storage, adaptation, or alteration of Data retrieved. Consultation, use disclosure by transmission, dissemination or otherwise making available alignment or combination restriction, erasure or destruction of Data as described under Article 4 (2). These processes apply to both electronic and manual data.

Special Categories of Personal Data Article 9 (1) GDPR Regulations:

Article 9 (1) Relates to the processing of Personal Data, notably Special Category Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or Trade Union Membership. The processing of generic Data, biometric Data for the purpose of uniquely identifying a natural person. Data concerning health, a natural person's sex life or sexual orientation is prohibited under Article 9. There are a number of exceptions to processing which are contained / outlined in Paragraph 1. They are also contained in Paragraphs 2 of 3 Article 9 and in Article 6 (1) sub sections (a) to (e) of the GDPR Regulations 2018.

5 PRINCIPLES OF DATA PROTECTION/DATA QUALITY PRINCIPLES

Principles of Data Protection Laws - Article 5

Article 5 contains seven principles relating to the Processing of Personal Data. They are also known as the Quality Principles of Data Protection.

It should be noted that all Personal Data / Special Category Data processed and retained by Westdoc in the course of its work is necessary and for the service it provides. This data is and will be dealt with and processed in compliance with the principles relating to processing Personal Data as prescribed in Article 5 of the General Data Protection Regulations GDPR 2018

All Personal Data shall be processed in accordance with the following principles:

1. Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.
2. Personal Data must be collected for specified, explicit and legitimate purposes and shall not to be processed in a manner or in ways incompatible with those purposes.
3. Data should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
4. Data should be kept accurate and up to date.
5. Data should not be kept longer than necessary.
6. Data must be kept safe and secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
7. The Data Controller must take into consideration people's rights.

Data in this Policy means and applies to Personal and Sensitive Data under Article 9 (1).

Westdoc as a Service Provider / Corporate Entity is committed to protecting Personal Data / Special Category Data as enshrined in the second title (Freedoms) of the Charter of Fundamental rights of the European Union which has full legal effect and applicability from the 11.12.2018

6 PURPOSE OF INSTALLING CCTV FOOTAGE

Westdoc operates in a highly controlled and regulated environment. With this in mind CCTV installation and footage is legitimate and necessary for a variety of reasons:

1. CCTV cameras are legitimate in the security of premises and Treatment Centres. Medication is stored and used in these Centres and the use of CCTV is important in securing and keeping the premises safe and secure.
2. CCTV is an important support for staff, some of which work in the overnight Treatment Centres.
3. CCTV footage is important for the prevention and detection of a crime.

Westdoc as a Data Controller is mindful of concerns and recognises that CCTV can be an intrusion into Data Protection and Privacy laws of individuals. Measures are carefully considered to ensure that monitoring or surveillance is not excessive. The use of CCTV is necessary for the welfare and safety of all Staff, Doctors and service users.

7 CCTV CHECKLIST

In advance of the installation of any CCTV system, careful consideration is given to the following matters.

1. The purposes of CCTV have been clearly defined and the footage is used for security and safety concerns. The data collected is used to re-enforce this.
2. CCTV footage processes Data and retains patient Data under the lawful processing exemptions contained in Article 6 (1) of the GDPR Regulations and under Article 2 of the Regulations 2018.
3. It is necessary to have CCTV footage in order to ensure staff safety and patient security and wellbeing.
4. Proactive measures to ensure proportionality in the use and positioning cameras is used by Westdoc. CCTV camera are located at the entrance point to the Treatment Centres. They are located near sensitive areas, notably, medicine cabinets. No cameras are situated in private areas such as toilets and changing areas.
5. Measures are in place to ensure that CCTV records are safe and secure from a technical and organisational perspective. Access to the recordings is limited to those who need to process them on a disclosure access claim.

6. Recordings are kept for no longer than necessary, namely, 30 days. The information recordings are automatically deleted after this period unless there is an access request to preserve the footage for a particular reason. The footage is deleted at the expiry of the specific purpose.
7. Recordings can be accessed by Data Subjects and by lawful enforcement Authorities upon receipt of a formal / written request to the Data Protection Officer at Westdoc.

8 DATA PROTECTION BY DESIGN AND DEFAULT

Westdoc as a Data Controller adheres to the principle of Data Protection by design and by default. Appropriate measures are in place which respects individual rights and privacy. Privacy and by default ensures that Data Protection settings are user friendly and only data necessary for specific processing purposes is adhered to and retained. Westdoc retains data for the shortest period necessary to achieve the purpose for which the system was installed to allow the Controller enough time to review any footage as necessary before deleting the data. The recording device (system is reviewed on a regular basis to ensure that data CCTV footage is retained no longer than necessary)

Where footage has been identified that related to a specific incident a longer period of retention may be justifiable in relation to a particular section of footage. For example, footage in relation to the investigation of a workplace incident or accident or where the footage is required or maybe used as evidence in a criminal investigation / proceedings. Westdoc receives requests for particular footage on an ongoing basis. The footage which is the subject matter of the request is isolated and preserved securely until the proceedings / investigated are fully complete. Once this occurs the requisite footage is then securely destroyed.

9 RETENTION OF PERSONAL DATA

CCTV footage is retained for a period of 30 days after the event. This retention period has been deemed necessary and appropriate, for example, Section 8 of the Civil Liberty and Courts Act 2004 requires a 30-day retention period for the purposes of defending a potential personal injury claim.

CCTV footage is retained for a period of 30 days after the event and after 30 days the footage is automatically deleted. If a request is received for particular CCTV footage it is preserved until it is deemed no longer necessary.

10 CCTV IN THE WORKPLACE

Westdoc has very legitimate reasons for installing CCTV cameras in the workplace. Employees also have legitimate expectations that their privacy will not be intruded upon disproportionately. Westdoc's cameras are focussed upon particular areas of risk, they are avoided where employees have increased privacy expectations such as break rooms, changing rooms and toilets. Clear notification is given to employees where CCTV monitoring is taking place. The monitoring is justified for the purposes of security, health and safety. However, there may be instances where the employer needs to use CCTV footage for a purpose other than one identified at the outset such as to investigate an allegation of gross misconduct or another disciplinary matter. It may be legitimate to monitor with CCTV in these situations. However, it is carried out on a case-by-case basis and it is justified out of necessity and proportionality in order to achieve a given purpose. A case should be made to demonstrate that the use of CCTV footage is necessary to provide evidence in a disciplinary matter and that access to CCTV is necessary to provide evidence in a disciplinary matter. In these limited circumstances (case the employees Data Protection rights should not be seen as presenting a barrier to the investigation of serious incidents.

11 DISCLOUSRE OF CCTV FOOTAGE TO THIRD PARTIES

There are occasions where Westdoc as a Data Controller is requested to disclose CCTV recordings to Third Parties for a purpose other than that for which it was originally obtained. For example, this may arise when a request is received from An Garda Síochána or another law enforcement body to provide footage to assist in the investigation of a criminal offence. Requests can be received by GSOC, Insurance companies, a request from a Solicitor, to preserve the locus of an accident scene. Such requests for copies of CCTV footage must be received in writing on foot of a formal request.

In the majority of cases, they relate to the investigation of a criminal matter. In the case of an emergency, a request may be received verbally and it may be sufficient to allow the release of material. However, this must be promptly followed up in writing for the purposes of accountability a record of all such requests is maintained by Westdoc as a Data Controller.

12 PROVIDING ACCESS TO CCTV FOOTAGE TO DATA SUBJECTS

Data Protection Law provides a right of access by Data subjects to their personal data. This applies to any individual who is identifiable from the image which has been recorded by a CCTV system. Westdoc upon receipt of a Data Access / CCCV Footage Request deals with this within one month, provided the scope of the request is no unduly large. In this event, it might take slightly longer. The data subject is contacted and advised of this. As a Data Controller Westdoc deal with all requests without undue delay.

In certain situations in order to facilitate the processing of such a request, the Controller may ask the individual applicant to indicate the date and time of the requested footage being requested. The majority of requests contain CCTV footage applications which are too wide and not directly relevant to the request itself. It is important to narrow the scope of the footage being sought and to ensure the relevant footage can and is provided.

If the CCTV footage request is received after the retention period the footage will have already been deleted on the date of the request. The Data Subject or the Agent acting on his /her behalf will be advised of this and that the footage no longer exists. If the access request has been received within the defined retention period the footage should not be delated until the request has been fulfilled.

Responding to access requests usually involves providing a copy of the footage in video format on a disc or memory stick. Any information disclosed should state the legal basis justifying the disclosure. Where the CCTV footage is technically incapable of being copied onto another device or in exceptional circumstances, It may be acceptable / permissible to provide picture stills for the duration of the recording in which the requested image appears in order to comply with the obligation to supply all the personal data held. There may be other parties which appear on CCTV footage. in certain situations. This may be difficult in the absence of appropriate technology for the data controller to pixelate or otherwise de-identity a particular image or other identifiable parties before supplying a copy of the footage to the requester. Alternatively, the data controller may seek the consent of all the other parties whose images appear in the CCTV footage.

Information in relation to Data Access Request application is contained in Westdoc's Data Protection Policy which can be accessed from its website at www.westdoc.ie It is available to members of the Patients if they wish to make data access requests.

13 COVERT SURVEILLENCE

The use of recording mechanisms to obtain data without an individual's consent is generally unlawful. Covert surveillance is permitted and normally only in exceptional

circumstances and on a case by case basis where data is being kept for the purposes of preventing, detecting or investigating offences or in relation to the apprehension or in the prosecution of offences. This provision implies that there is a written policy which justifies the procedure, measures and safeguards that are implemented with the objective of the Gardaí becoming involved or another prosecution regarding other authorities in relation to a potential criminal investigation or civil legal proceedings.

A Data Protection Impact Assessment (DPIA) should be carried out prior to the installation of any covert systems to clear up access whether or not the measures can be justified on the basis of necessity and proportionality in order to achieve the purpose.

14 FACIAL RECOGNITION AND BIOMETRIC DATA

Certain specific technical features in relation to certain CCTV systems and the use of facial recognition software can be a factor in determining the basis on which data can be lawfully processed. It should be noted that facial recognition processing and accordingly the data processed is “Article 9 – Special Category Data” which is subject to GDPR requirements.

15 DATA PROTECTION IMPACT ASSESSMENT DPIA

The Data Protection Impact Assessment DPIA is required to be carried out by an Organisation under Article 35 (1) of the GDPR Regulations 2018 where processing is likely to result in a high risk to the freedoms of the Data Subject. A DPIA can be used to identify and mitigate against any Data Protection Regulation risks arising from a new project under the GDPR Regulations. DPIA’s are mandatory for any new high-risk processing activities / projects. If a new set of cameras are being installed and if an additional area needs to be monitored a DPIA should be carried out before this new activity is engaged.

16 Points of Contact

Data Subjects can contact Westdoc Ltd. Unit 18, Liosban Business Park, Tuam Road, Galway.

If you wish to make an access request or exercise your rights as outlined under Data Protection Law or if you have any queries, please contact the Data Protection Officer at Westdoc.

Email:	matt@westdoc.ie
Phone:	064 6691974
Postal Address	Data Protection Officer, Unit 18A, Liosban Business Park, Tuam Road, Galway H91 FW13

Further information is available on the Westdoc website: www.Westdoc.ie

17 Further information

If you require further information on Data Protection, please contact the Offices of the Data Commissioner (The Supervisory Authority)

Lo Call Number	1890 252 231
Email	dpo@dataprotection.ie
Postal Address	Data Protection Commissioner, Canal House, Station Road, Port Arlington, Co Laois R32 NP 23