

University of the Philippines Diliman
DATA PROTECTION TEAM

MEMORANDUM

Reference No. DPT 18-07

FOR : [Redacted]
[Redacted]

[Redacted]
[Redacted]

[Redacted]
[Redacted]
[Redacted]

SUBJECT : **Use of CCTV and Orientation on Social Media and Privacy Laws**
DATE : 20 April 2018

Dear [Redacted] and [Redacted]:

We render an advisory opinion on use of Closed-Circuit Television (CCTV) cameras in the [Redacted] and the social media and privacy laws your good faculty and staff should be aware of.

Opinion

A privacy notice should be posted in all entry points of [Redacted] stating that the identity, actions, and whereabouts of all individuals in and around the premises of the building are being captured and recorded by CCTV cameras and that by entering the premises, the individual consents to CCTV-related processing of his or her personal information. The suggested wording for this notice is found below.

The Data Protection Team will send a representative to hold a seminar privacy laws applicable to [Redacted] administrative and academic operations. This will include privacy laws relevant to social media use. However, for other social media laws such as identity theft and libel, we kindly refer the matter to the [Redacted] as these are beyond data privacy matters.

Discussion

I. CAPTURING OF CCTV FOOTAGES

CCTVs capture and record visual images. These visual images are information which can be used to identify people. As such, CCTV recordings are considered personal information. The Data Privacy Act of 2012 defines personal information as:

“Section 3. Definition of Terms.

x x x

(g) Personal information refers to any information whether recorded in a material form or not, from which **the identity of an individual is apparent or can be reasonably and directly ascertained** by the entity holding the information, or when put together with other information would directly and certainly identify an individual.”

[Emphasis supplied]

As personal information, [Redacted] has the following obligations with respect to the CCTV recordings:

- (1) Use CCTV recordings strictly for security purposes only;
- (2) Obtain consent of individuals entering and around the premises;
- (3) Inform individuals of the purpose and retention period of the CCTV recordings; and
- (4) Restricted Access to and Security Clearance for CCTV recordings.

Use CCTV recordings strictly for security purposes only

Personal information such as CCTV such as recordings which identify the identity of individuals cannot be processed without a ***legitimate purpose***. The [Redacted] may capture CCTV footages for the legitimate purpose of maintaining security within and around its premises. Since this is the legitimate purpose that justifies the act of CCTV recording, [Redacted] may not use CCTV recordings for any other reason.

There should be no attempt at identifying the individuals captured on CCTV unless it is related to a security matter.

Obtain consent of individuals entering and around the premises and Inform individuals of the purpose and retention period of the CCTV recordings

The consent of an individual must be obtained prior to or as soon as practicable after any footage is recorded. Prior to obtaining this consent, the individual must be informed of the ***purpose*** and retention ***duration*** of the CCTV recordings.

To this end, it is suggested that a CCTV Privacy Notice be posted in **all** the following:

- (1) Entry points in and around the building; and
- (2) Receiving areas where security guards require visitors to log their information.

The following privacy notice is suggested:

<p>CCTV Privacy Notice</p> <p>For security purposes, this building and its surrounding premises are monitored by Closed Circuit Television (CCTV) cameras which capture, record for thirty (30) days, and share to relevant units footages which determine your identity, actions, and whereabouts. Your footage may be recorded for a longer duration and processed other manners if it may be of use to or involved in a security matter.</p> <p>By entering these premises, you agree to the capture, recoding, processing, and sharing of all information directly and indirectly obtained by CCTV cameras.</p>
--

Parking lots and external waiting areas which are CCTV-monitored should also have a CCTV Privacy Notice.

In all receiving areas where visitors log their information, the following suggested to be posted near or on the logbook or e-logbook:

<p>Notice</p> <p>By indicating your details in this logbook or entering these premises, you undertake to have read, understood, and consented to our CCTV Privacy Notice.</p>
--

Restricted Access to and Security Clearance for CCTV recordings

As a government agency and no less than the country's national university, the University is covered by the National Privacy Commission (NPC) Circular on Security of Personal Data in Government Agencies.

This NPC Circular requires that there should be appropriate *security clearance* to all data centers used to store CCTV recordings. This should be enforced by an *access control system* that records when, where, and by whom the data centers are accessed. Access records and procedures should be reviewed by [Redacted] management regularly.

As a government agency, [Redacted] should strictly regulate access to personal data under its control or custody. It should grant access to personnel through the issuance of a *security clearance*¹ by the head of [Redacted]. A security clearance should only be issued to personnel whose access is indispensable to the security purpose of capturing CCTV footages. Copies of issued security clearances should be filed with the University's Data Protection Team.

II. DISCUSSION OF DATA PRIVACY LAWS TO [Redacted]

The Data Protection Team will send a representative to hold a seminar on privacy laws applicable to [Redacted] administrative and academic operations. We kindly request that your point person for this seminar coordinate the schedule with us by sending an email to dpo.updiliman@up.edu.ph. We can either send a representative of the Data Protection Team if the seminar will be on a weekday or the University's Data Protection Officer if the seminar will be on a weekend. The seminar will include privacy laws relevant to social media use.

For other laws governing social media such as cracking, identity theft, and libel, we kindly refer the matter to the [Redacted] as these are beyond data privacy matters and are governed by other laws.

Please feel free to reach out for clarifications or further inquiries.

Yours Truly,

Elson B. Manahan
Data Protection Officer
University of the Philippines Diliman

Confidentiality

This document, its contents, and any attachments included are privileged, confidential, and exclusively for the intended recipient. No part of this document may be reproduced or exhibited without the written consent of the UP Diliman Data Protection Officer. In case of wrongful receipt of or unauthorized access to this material, please immediately inform the author and permanently delete the wrongfully received copy.