

2016

# Data Protection Law

LEGAL PRINCIPLES OF COMPUTER FORENSICS  
SAMANTHA SHEEHAN

WATERFORD INSTITUTE OF TECHNOLOGY | Computer Forensics and Security

## Declaration

**I declare that the work which follows is my own, and that any quotations or paraphrasing from any source is clearly identified and referenced. I have read and understood the WIT Anti Plagiarism Policy and understand the consequences of plagiarism.**

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_

## Contents

Cases .....	2
Introduction .....	3
Irish Laws and Guidelines Surrounding Data Protection .....	4
Irish Banks Ltd. ....	7
(a) The use of CCTV footage .....	8
(b) John's Legal Rights .....	10
Conclusion.....	12
Bibliography .....	13

## Cases

*The Data Protection Commissioner – Case Study 10* accessed at  
<https://www.dataprotection.ie/docs/Case-Studies-2008/939.htm#10>

*Karen Deegan v Dunnes Stores* reported by the Irish times at  
<http://www.irishtimes.com/news/crime-and-law/dunnes-stores-monitored-staff-suspected-of-stealing-goujons-1.1770261>

And the Independent at  
<http://www.independent.ie/irish-news/courts/dunnes-employee-sacked-for-eating-chicken-goujons-at-work-tribunal-told-30041889.html>

*Rozbicka v Dunnes Stores* reported by The Independent at  
<http://www.independent.ie/irish-news/courts/dunnes-stores-boss-secretly-monitored-his-staff-for-77-days-26793139.html>

*Barry Hayden v DPP* reported by the Irish Times at  
<http://www.irishtimes.com/news/prison-officer-accused-of-assault-fails-to-stop-case-1.461388>

## Introduction

The general stance on privacy in Irish law seems to be about balance, yes, we have a right to privacy but only to a certain extent. The data protection laws mirror this sentiment with a heavy reference toward proportionality, giving a Judge discretion in decisions made in this regard. However, with the increased digital presence in Ireland, digital privacy is becoming a hot topic. One notable case which indicates a shift in opinion is *Schrems v DPP*, where the Court of Justice of the European Union (CJEU) ruled the Safe Harbour Agreement with the U.S. illegal, leaving Europe in unknown territory. A new agreement has been drawn up, however the most interesting thing about the case is the decision itself, which seems to indicate a more serious view being taken on privacy and the mass collection of personal data. Although with the decision being relatively new, we will have to wait and see how this precedent will be put to use in Irish court adjudications, making it an exciting time for data protection in Ireland. For now, however, data protection in Ireland is governed by the Data Protection Act, 1988 and the Data Protection Amendment Act, 2003.

## Irish Laws and Guidelines Surrounding Data Protection

The use of CCTV in the workplace is governed by the same data protection laws which protect John's rights, the Data Protection Act, 1988<sup>1</sup> and the Data Protection Amendment Act, 2003<sup>2</sup>. The basic principle behind the Acts is the protection of personal data and right to privacy of each individual.

In the Act data is described as

*"data"* means information in a form in which it can be processed".

The term "personal data" is used frequently and is described by the Data Protection Commissioner as<sup>3</sup>:

"personal data" means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller".

The Act uses terms such as "data subject", "data controller", and "data processor", to define the entities involved in processing such data, they are defined in the Act as follows:

*"data subject"* means an individual who is the subject of personal data"

*"data controller"* means a person who, either alone or with others, controls the contents and use of personal data"

*"data processor"* means a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment"

The Act is responsible for the creation of the Data Protection Commissioner's office and lays out the details of his role, responsibilities and authorities concerning data protection. Per his website<sup>4</sup> his main role is enforcing the law with respect to the rights to privacy of individuals laid out in the Acts. The Data Protection Commissioner is appointed by the Government and works independently to ensure a fair process.

---

<sup>1</sup> The Data Protection Act 1988

<sup>2</sup> The Data Protection Amendment Act 2003

<sup>3</sup> Data Protection Commissioner -What is personal data?

<sup>4</sup> Data Protection Commissioner- About us

Section 2<sup>5</sup> of the Act lays out provisions for the collection, processing, storing and use of personal data by a data controller, Section 2(c) describing the limitations of data collection and storage:

(c) the data—

- (i) shall be kept only for one or more specified and lawful purposes,
- (ii) shall not be used or disclosed in any manner incompatible with that purpose or those purposes,
- (iii) shall be adequate, relevant and not excessive in relation to that purpose or those purposes, and
- (iv) shall not be kept for longer than is necessary for that purpose or those purposes

These provisions are important for data controllers to follow strictly, and these laws are enforced by the Data Protection Commissioner.

Also, included in this section is information on limitations of the Act in relation to personal data such as:

(5) (a) *Paragraph (c) (iv) of the said subsection (1) does not apply to personal data kept for historical, statistical or research purposes, and*

(b) *the data or, as the case may be, the information constituting such data shall not be regarded for the purposes of paragraph (a) of the said subsection as having been obtained unfairly by reason only that its use for any such purpose was not disclosed when it was obtained*

if the data are not used in such a way that damage or distress is, or is likely to be, caused to any data subject.

This Section also lays out guidelines specific for data collected and processed for advertising purposes.

Sections 3<sup>6</sup> and 4<sup>7</sup> deal with an **individual's rights to establish the existence of personal** data, and access to that data, simply meaning any individual has a right to find out if information is being stored about them, and also have a right to procure said data. If a company/entity is withholding, a written request can be made and the data must be sent within 21 days<sup>8</sup> in all cases except where restrictions are placed in Section 5<sup>9</sup>.

---

<sup>5</sup> The Data Protection Act 1988, Section 2

<sup>6</sup> The Data Protection Act 1988, Section 3

<sup>7</sup> The Data Protection Act 1988, Section 4

<sup>8</sup> The Data Protection Commissioner – Making an Access Request

<sup>9</sup> The Data Protection Act 1988, Section 5

Section 6<sup>10</sup> is in relation to the right to rectify or erase personal data as appropriate, which can be requested in written form and must be completed by the data controller within 40 days of the request. This is meant to comply with the right to have personal data be accurate.

Section 7<sup>11</sup> of the Act is in relation to a duty of care afforded to a data subject by the data controller or data processor, simply meaning the data controller or processor must take responsibility for the personal information it retains.

According to the Data Protection Commissioner<sup>12</sup>, when an entity requires personal data to be collected, retained, or used it must first meet the requirements set out in the Act in order to be in compliance with the law.

If a data subject has a complaint or issue with regard to a data controller or data processor it is the responsibility of the Data Protection Commissioner to investigate and, if necessary, discipline the data controller or data processor involved in said complaint<sup>13</sup>.

---

<sup>10</sup> The Data Protection Act 1988, Section 6

<sup>11</sup> The Data Protection Act 1988, Section 7

<sup>12</sup> The Data Protection Commissioner – Responsibilities of Data Controllers

<sup>13</sup> The Data Protection Commissioner – Enforcement

## Irish Banks Ltd.

John and Mary have been in a relationship for two years. Mary works for Irish Banks Ltd. John has an account with the bank. Mary is suspicious that John has been going out with his friends when he is supposed to be in work. She decides over a two-week period to check his account number to see if there are any unusual transactions or withdrawals to build her case against John. She finds that he used his card in a local pub one night. Armed with this compelling evidence she confronts him and ends the relationship. John is furious and makes a complaint to the Bank arguing that his data protection rights and privacy rights have been infringed. The Bank now seeks your advice on the following.

(a) They have CCTV footage of Mary on the computer at the relevant time. They seek your advice as to whether the footage can be used in disciplinary or court proceedings against her. There are no signs that cameras are operating in the business centre at the Bank.

(b) They seek your advice as to whether John's data protections rights have been infringed. If so why?

Advise the Bank.



### (a) The use of CCTV footage

CCTV footage is considered in Irish law to constitute personal data, as such in this scenario Irish Banks Ltd are considered to be the “data controllers” while Mary would be the “data subject”. Under the Data Protection Act, 1988<sup>14</sup> there are strict laws against the harvesting of personal data. The Data Commissioner describes how this is interpreted regarding surveillance in the workplace<sup>15</sup>, and more specifically CCTV. The most noticeable issue in this regard is proportionality, that is maintaining a balance between an employer’s right to run an efficient business and an employee’s right to privacy. To maintain this balance guidelines have been put in place which employers must adhere to in order to operate within the confines of the law<sup>16</sup>.

In a case study<sup>17</sup> published by the Data Protection Commissioner in 2008 an employer tried to use illegally collected CCTV footage for disciplinary action. An employer had attempted to use CCTV footage to log entry and exit from the place of employment for a few employees. The Commissioner was contacted by two of the employees who claimed that they had never been informed of the purpose of the cameras, nor was there sufficient signage indicating the use of CCTV. The Data Commissioner, upon receiving the complaint, outlined the law regarding CCTV footage to the employer in a letter:

“to satisfy the fair obtaining principle of the Data Protection Acts with regard to the use of CCTV cameras, those people whose images are captured on camera must be informed about the identity of the data controller and the purpose(s) of processing the data.”

And further explained to the employer that to achieve this they must use proper signage in prominent locations, and if the footage is for the purpose of employee monitoring, employees must be informed beforehand. The employer withdrew from their actions against the employee’s as the CCTV footage could not be relied on as evidence.

Another case brought before the Employment Appeals Tribunal (herein referred to as the EAT) reflected the decision of the Data Commissioner when a Dunnes Stores employee filed a case for unfair dismissal. The employee was fired after being captured on CCTV eating goujons without paying for them. The security guard confirmed at the hearing he had installed two covert CCTV cameras in the store’s deli without the employee’s knowledge. The EAT found Dunnes Stores investigation “*fell short of acceptable practice*” and awarded the woman eight thousand euro<sup>18</sup>.

The relevance of the Act in this particular situation, is unless these guidelines were followed the CCTV images captured by Irish Banks Ltd were collected illegally. In this case the signage surrounding the CCTV cameras were insufficient, meaning this data could not be used by the bank for any purpose. The Data Commissioner’s case study, however is a simple matter of internal disciplinary action, and although the logic in this instance is correct, the courts don’t always seem to have the same opinion.

---

<sup>14</sup> The Data Protection Act, 1988

<sup>15</sup> The Data Protection Commissioner – Surveillance in the Workplace

<sup>16</sup> Citizens Information – Surveillance of Electronic Communications in the Workplace

<sup>17</sup> The Data Protection Commissioner – Case Study 10

<sup>18</sup> The Irish Times – Dunnes Stores Monitored Staff Suspected of Stealing Goujons

T.J. McIntyre makes several good points in his blog post from November 2011<sup>19</sup>, and points to cases where the outcome was different. One such case was an EAT hearing where an employee claiming she was fired wrongfully by Dunnes Stores for several breaches, including clocking in and out and food hygiene breaches, CCTV recordings were used to prove the employees wrong-doing. The case was reported by The Independent<sup>20</sup> in 2011 in a piece alleging the employees working in Dunnes at the time were being secretly monitored for seventy-seven days. Certain details of the hearing were unclear, such as whether the CCTV cameras themselves were hidden or if it was the purpose of the cameras which were hidden from the staff. Also, no formal judgement was written so the outcome of the case was unclear, however it appears that the illegality of the cameras never became a topic in the hearing.

Following on from this case in 2012 The Irish Times<sup>21</sup> reported on a High Court decision to allow the use of illegally obtained CCTV footage in the case of a prison officer allegedly assaulting an inmate of St. Patricks Institution for Young Offenders. As part of his defence the prison officer argued there should have been notices about the use of CCTV cameras and claimed that his data protection rights had been breached. Justice George Birmingham ruled that the prison officers case was “devoid of merit”, however with no formal written judgement Justice Birmingham’s reasoning is uncertain.

In regards to the instance of Irish Banks Ltd, it is my opinion that without distinct and apparent signage and staff awareness of the camera’s location and purpose the collection and use of Mary’s personal information is illegal. However, the law as it stands allows a Judge to use their discretion when dealing with these cases as proportionality is a huge factor of determining wrong-doing. As the court tends to sway on the side of inclusiveness I would recommend the use of the CCTV footage to pursue action against Mary. With the High Court ruling setting a legal precedent, there is little reason to consider an alternative.

---

<sup>19</sup> TJ McIntyre – Is Illegally Obtained CCTV Footage Accepted in Court?

<sup>20</sup> The Independent– Dunnes Stores Boss Secretly Monitored His Staff for 77 Days

<sup>21</sup> The Irish Times – Prison Officer Accused of Assault Fails to stop case

## (b) John's Data Protection Rights

It is my opinion that John's data protection rights were not breached by Irish Banks Ltd.

According to the Data Commissioner<sup>22</sup> the rights of a "data subject" (John) are as follows

1. The right to be informed
2. The right of access
3. The right of rectification or erasure
4. The right to block certain uses
5. The right to have your name removed from direct marketing lists
6. The right to object
7. The right to have your data processed in accordance with the data protection acts

To explain the right to have your data processed in accordance with the data protection Acts:



### *1. Right to have your data processed in accordance with the Data Protection Acts*

Those holding data relating to you are obliged to:

- obtain and process the information fairly
- keep it only for one or more specified, explicit and lawful purposes
- use and disclose it only in ways compatible with these purposes
- keep it safe and secure
- keep it accurate, complete and up-to-date
- ensure that it is adequate, relevant and not excessive
- retain it no longer than is necessary for the purpose or purposes
- give you a copy of your personal data, on request.

---

<sup>22</sup> The Data Commissioner – A guide to Your Rights accessed

In my opinion Mary broke the law under section 21 of the Act aimed specifically at employees:

“**21.**—(1) Personal data processed by a data processor shall not be disclosed by him, or by an employee or agent of his, without the prior authority of the data controller on behalf of whom the data are processed.

(2) A person who knowingly contravenes *subsection (1)* of this section shall be guilty of an offence.”<sup>23</sup>

However Irish Banks Ltd. did not breach data protection laws, even if it is the case that Mary broke the law, John’s rights, the right to access and erasure and other rights laid out by the Data Commissioner remained intact. Irish Banks Ltd. obtained and processed the information fairly, kept it for a specified purpose, used and disclosed it in ways compatible with those purposes and so on. Mary acted outside the authority of Irish Banks Ltd. Meaning while it was immoral, illegal and simply wrong for Mary to access John’s personal data, John’s rights under the law were not infringed.

---

<sup>23</sup> The Data Protection Act, Section 21 accessed at

## Conclusion

Where the laws regarding data protection are concerned, Judges in Ireland are given some leeway to decide on proportionality, and reasonable use. This, in my opinion, is a good system. Judges have the experience and knowledge required to make a sound weighted decision. Data protection laws in Ireland are changing due to some of these decisions setting legal precedent, and with the exponential growth of digital data these changes couldn't have come at a better time.

## Bibliography

The Data Protection Act 1988 accessed at

<http://www.irishstatutebook.ie/eli/1988/act/25/enacted/en/print#sec2>

The Data Protection Amendment Act 2003 accessed at

<http://www.irishstatutebook.ie/eli/2014/si/338/made/en/print?q=data+protection>

Data Protection Commissioner -What is personal data? Accessed at

<https://www.dataprotection.ie/docs/What-is-Personal-Data/210.htm>

Data Protection Commissioner- About us

<https://www.dataprotection.ie/docs/About-the-office-of-the-DPC/b/1032.htm>

The Data Protection Commissioner – Making an Access Request accessed at

<https://www.dataprotection.ie/docs/Making-an-Access-Request/963.htm>

The Data Protection Commissioner – Responsibilities of Data Controllers accessed at

<https://www.dataprotection.ie/docs/Responsibilities-of-data-controllers/1243.htm>

The Data Protection Commissioner – Enforcement accessed at

<https://www.dataprotection.ie/docs/Enforcement/b/1009.htm>

The Data Protection Commissioner – Surveillance in the Workplace accessed at

[http://www.citizensinformation.ie/en/employment/employment\\_rights\\_and\\_conditions/monitoring\\_and\\_surveillance\\_at\\_work/surveillance\\_of\\_electronic\\_communications\\_in\\_the\\_workplace.html](http://www.citizensinformation.ie/en/employment/employment_rights_and_conditions/monitoring_and_surveillance_at_work/surveillance_of_electronic_communications_in_the_workplace.html)

Citizens Information – Surveillance of Electronic Communications in the Workplace accessed at

[http://www.citizensinformation.ie/en/employment/employment\\_rights\\_and\\_conditions/monitoring\\_and\\_surveillance\\_at\\_work/surveillance\\_of\\_electronic\\_communications\\_in\\_the\\_workplace.html](http://www.citizensinformation.ie/en/employment/employment_rights_and_conditions/monitoring_and_surveillance_at_work/surveillance_of_electronic_communications_in_the_workplace.html)

The Data Protection Commissioner – Case Study 10 accessed at

<https://www.dataprotection.ie/docs/Case-Studies-2008/939.htm#10>

The Irish Times – Dunnes Stores Monitored Staff Suspected of Stealing Goujons accessed at

<http://www.irishtimes.com/news/crime-and-law/dunnes-stores-monitored-staff-suspected-of-stealing-goujons-1.1770261>

TJ McIntyre – Is Illegally Obtained CCTV Footage Accepted in Court? accessed at

<http://www.tjmcintyre.com/2011/11/is-illegally-obtained-cctv-footage.html>

The Independent– Dunnes Stores Boss Secretly Monitored His Staff for 77 Days accessed at

<http://www.independent.ie/irish-news/courts/dunnes-stores-boss-secretly-monitored-his-staff-for-77-days-26793139.html>

The Irish Times – Prison Officer Accused of Assault Fails to stop case accessed at

<http://www.irishtimes.com/news/prison-officer-accused-of-assault-fails-to-stop-case-1.461388>

The Data Commissioner – A guide to Your Rights accessed at

[https://www.dataprotection.ie/documents/guidance/A\\_Guide\\_to\\_Your\\_Rights\\_web\\_version.pdf](https://www.dataprotection.ie/documents/guidance/A_Guide_to_Your_Rights_web_version.pdf)