***03.치안시책자료❹341~362 2005.2.23 10:29 AM 페이지341

時策

英國의 CCTV關聯 法規考察*

盧 鎬 來**

Ⅰ. 序 言

CCTV(Closed circuit television)에 의한 감시는 우리의 일상생활에서 크게 증가하고 있다. CCTV가 범죄예방과 축소에 어느 정도 효과적인가에 대한 논쟁이 계속 중이지만 한가지 확실한 것은 공공이 쉽게 접근할 수 있는 다양한 지역에 설치되고 있다는 것이다. 우리는 거리를 걸어가거나 은행이나 가게에 가게 될 때 철도역이나 공항을 통하여 여행할 때 CCTV에 촬영될 수 있다. 영국의 과학과 기술에 관한 왕립위원회(The House of Lords Select Committee on Science and Technology)는 CCTV에 대한 공공의 신뢰가 유지된다면 그 설치와 사용에 대해 엄격한 통제가 있어야 한다는 견해를 표명했다.

정보보호법(Data Protection Act 1998)이 발효하게 된 2000년 3월 1일에 이르러서야 공공지역에 대한 CCTV감시에 대해서 체계적인 법적 통제의 바탕이 마련되었다. 이러한 새로운 법률의 정의는 1984년의 정보보호법보다 더 넓고, 과거의 정보보호입법보다 CCTV카메라에 의해 촬영된 이미지처리에 더 쉽게 적용할 수 있다. 이 법규는 과거에 컴퓨터에서의 사적 정보처리에 적용되었던 정보처리기준과 마찬가지로 CCTV활용을 규제할 수 있다. 1998년 입법의 주요특징은 정보보호법 제51조 (3)(b)의 규정에 의해 정보관리책임자(Data Protection Commissioner)는 정보관리수칙(codes of practice)을 제정하여 반포하는 권한을 가지게 되었다. 의회에 대한

* 本稿는 영국의 Data Protection commissioner인 Elizabeth France가 2000년 7월에 작성한 "CCTV Code of Practice"를 번역하여 재구성한 것이다. 자료의 출처는 http://www.dataprotection.gov.uk/dpr/dpdoc.nsf/8a6242113a3c89f0802... (2003. 7. 8)임.

** 세명대학교 법정학부 경찰행정학과 교수(Rohtiger@semyung.ac.kr)

***03.치안시책자료❹341~362 2005.2.23 10:29 AM 페이지342

14번째 보고서(14th Annual Report to Parliament)에서 본인은 CCTV운영에 대한 가이드하는 규정을 만들 수 있는 권한을 가지게 되었다. 이러한 관리규정(Code of Practice)은 1998년 정보보호법에 따라[1] 첫 번째 반포한 Commissioner' s Code이다.

이 법규는 시민들이 자유롭고 제한없이 출입할 수 있는 지역에 대한 감시를 규제하고 있다. 1998년 정보보호법이 CCTV의 용도외의 사용을 규제하는 것이지만 본 CCTV관리원칙은 더 넓은 관심분야를 언급한다. 규정들의 대부분이 CCTV의 용도외의 사용과 관련될 것이고, 다른 안내지침을 만들 때 기준이 될 것이다. CCTV시스템 운영대표자들이 만든 기준들은 도움이 되지만 법적으로 효력이 없다. 이와 같은 자료보호입법의 변화는 최초로 개인에 대한 이미지의 수집과 처리에 적용되는 법적기준이 만들어졌다는 것을 의미한다.

본 규정(Code of Practice)은 CCTV운영자들에게 법적 의무를 이해시키고, 곳곳에 설치되어야 하는 안전장치에 관하여 시민들을 안심시키는 두가지 목적을 가지고 있다. 본 규정은 '98 자료보호법에 따라 취해야 조치에 대하여 규정하고 가이드라인을 제공한다. 본 규정은 자료보호법을 준수해야 하는 기준을 명확히 하고, 엄격한 법적 조건이 아니라 모범적인 사례를 제시한다.

이 규정이 반포되기 전에 본인은 정보통제자, 자료대상자에게 자문을 구하고, 본인의 website에 초안을 공개했다. 본인은 이 규정을 만들기까지 도움을 준 모든 사람들에게 감사를 드린다.

1984년의 정보보호법의 부족한 점으로는 자료통제자의 일상활동에 관련되어야 할 필요성이 제기되었고, 실제에 맞게 갱신되는 생생한 기록과 쉽게 알수 있는 법규가 필요하다.

이 규정은 변화하는 기술, 용도, 법체계에 맞도록 계속적으로 검토되어야 한다. 이러한 맥락에서 2000년 10월부터 적용되는 인간권리법(Human Rights Act 1998)은 개인에 대한 중요한 안전장치를 제공할 것이고, 이 규정을 검토할 때 해석의 기준이 될 것이다.

이 규정을 만든 본인의 바램은 CCTV운영자들이 1998정보보호법을 준수하고, 모범적 운영에 대한 기준을 지키도록 도움을 제공하는 것이다. 이 규정은 CCTV운영자의 사적 자료의 처리에 도움을 줄 뿐만 아니라 공공의 신뢰를 유지하는데에도 일조를 할 것이다.

1) section 51(3) (b) Data Protection Act 1998: the Commissioner considers it appropriate to do so, the Commissioner shall, after such consultation with trade associations, data subjects or persons representing data subjects as appears to him to be appropriate, prepare and disseminate to such persons guidance as to good practice.

II. CCTV 管理運營 基準

1. 설치전의 최초단계

CCTV를 설치하기 전에 사용자는 CCTV 설치의 목적을 설정하고, CCTV의 영상자료를 합법적으로 관리할 수 있는 CCTV 정보통제자가 선정되어야 한다. CCTV의 목적은 범죄의 예방 · 수사 · 탐지, 범법자의 체포 · 기소, 공공 및 종업원의 안전, 일정한 토지의 감시 등 다양하게 설정할 수 있다. 그 정보통제자는 자료보호원칙에 따라 합법적으로 처리하고 처리내용을 기록해야 한다.

2. 카메라의 설치

설치위치는 신중하게 고려되어야 한다. CCTV는 의도했던 목적 범위내의 공간만을 감시하는 방식이어야 하지만 부득이 CCTV설치지역이 가정의 정원과 같은 지역과 경계를 이루고 있고 그 지역까지 감시가 되고 있다면 그러한 공간의 소유자의 동의를 받아야 한다. CCTV 운영자는 설치목적만을 위해서 이미지를 사용해야 한다. 예를들면 CCTV의 촬영범위가 어느 특정인의 뒷마당까지 도달하는데 그 장소에서 일광욕을 하는 여성이 있는 경우가 있을 수 있고, 그러한 경우 운영자가 그 여성의 프라이버시를 침해하지 않도록 교육을 받아야 한다.

일반시민들이 감시장비가 설치된 지역에 들어가고 있다는 것을 알 수 있도록 표지판을 설치해야 하고, 그 표지판은 명확하게 볼 수 있고 읽기가 쉬어야 한다. 그리고 그 표지판에는 CCTV를 관리하고 시행하는 관할기관에 대한 정보가 기술되어 있어야 한다. 구체적으로 범죄예방과 공공의 안전을 위한 목적으로 설치되었으며 이 계획은 그 지역의 자치단체, 경찰서, 주민의 협력에 의해 관리되고 있다고 기재되어야 하며, 더 많은 정보를 알고 싶은 사람을 위해 전화번호를 기재할 필요성이 있다.

3. 이미지의 질

그 장비에 의해 산출된 이미지는 의도하는 목적을 달성할 수 있도록 양질의 화면을 제공해야

***03.치안시책자료❹341~362 2005.2.23 10:29 AM 페이지344

한다. 예를 들면 범죄를 탐지하고 예방하기 위해서 설치되었다면 이러한 목적에 충분하도록 화질이 좋아야 한다. 카메라는 명확한 이미지를 기록할 수 있도록 적절하게 관리되어야 하고, 외부의 충격이나 파괴에 훼손되지 않도록 보호되어야 한다.

4. 이미지의 처리

설치목적에 부합하지 않는 이미지는 필요이상의 기간동안 보관되지 말아야 한다. 그 이미지가 보관될 경우 증거가치를 높이고, 촬영된 사람들의 인권을 보호할 수 있도록 철저하게 관리되어야 한다. 그 이미지에 대한 접근과 보관은 1998년 법의 조건에 따라 통제되어야 한다. 보관기간은 필요성에 따라 1개월 혹은 3개월까지 보관해야 할 경우도 있다. 소송이 제기되어 증거로 제시해야 할 경우 그 기간이 길어질수 있다. 예를 들면 자동현금인출기로부터 기록된 이미지는 고객과의 분쟁을 대비하기 위해서 3개월 동안 유지 보관될 필요성이 있다. 왜냐하면 이 3개월이라는 보관기간은 개인이 그들의 출금명세서를 받는 기간을 의미한다. 보관기간이 만료되는 즉시 폐기되어야 한다. 그 이미지가 증거로 보관된다면 외부로부터 접근이 차단된 곳에 보관되어야 한다. 그리고 이미지가 경찰관에게 전달된 경우 운영자는 그 경찰관의 이름과 경찰서를 기록하고 경찰관의 서명을 받아두어야 한다. 모니터의 재방영은 프라이버시의 침해 가능성이 있으므로 권한있는 당사자 이외에는 볼 수 없도록 해야 한다. 그 기록이미지에 대한 접근은 제3자의 열람요청이 있을 경우 허용여부를 결정할 수 있는 관리자 혹은 지정된 사람에 한정하여 이루어져야 한다. 녹화된 이미지의 검토는 관리자 혹은 지정된 관리자가 참여하는 사무실같은 지역에 한정되어야 한다.

5. 이미지에 대한 제3자의 접근성과 공개

CCTV와 유사감시장비에 의해 기록된 이미지에 대한 접근과 공개는 개인의 권리가 보장되고, 이미지가 증거목적으로 사용되는 경우 증거는 손상되지 않은 상태로 보존될 수 있도록 관리되어야 한다. CCTV의 사용자들은 이미지를 복사하여 공개하는 경우 그 이미지를 얻으려는 목적 혹은 이유와 배치되지 않아야 한다. 이러한 원칙은 제7, 8 정보보호원칙에 의한 것이고, '98정보보호법 해설부분에서 토론될 것이며, 이러한 원칙에 필요한 기준은 다음과 같다. 모든 종업원들은 기록된 이미지의 접근, 공개에 대한 제한사항을 알아야만 한다.

1) 기록된 이미지에 대한 접근은 그 장비를 사용하는 목적달성을 위해서 접근이 필요한 직원에 한정되어야 한다.
2) 이미지가 기록되는 매개체에 대한 접근이 있을 경우 모두 기록되어야 한다.
3) 제3자에게 그 이미지를 공개할 경우에는 다음과 같은 한계가 있다.
   - **예를들면 – 그 시스템의 목적이 범죄의 예방과 탐지에 있다면 제3자에 대한 공개는 다음과 같이 제한되어야 한다.**
     - **범죄를 수사하는 법집행기관**
     - **소추기관**
     - **관련법률 대표자들**
     - **언론, 범죄사건에서 피해자와 목격자, 범죄자를 확인하기 위해 공공의 신고가 필요한 경우, 이 때에도 피해자의 의사가 고려되어야 한다.**
     - **이미지를 관리하고 유지하는 사람들(공개가 범죄수사 혹은 범죄소추에 편견을 야기하는 것이 아니라면)**
4) 모든 접근과 공개 요청은 기록되어야 한다. 접근과 폭로가 부인된다면 그 이유가 기록되어야 한다(제7 정보보호원칙).
5) 그 이미지에 대한 접근과 공개가 허용된다면 다음 사항이 기록되어야 한다.
   - **a) 접근이 허용된 날짜와 시간 혹은 공개한 날짜**
   - **b) 접근과 공개가 허용된 제3자의 확인**
   - **c) 접근과 공개가 허용된 이유**
   - **d) 접근과 공개되는 정보의 범위(이 부분은 제3자에 대한 접근과 공개부분을 참조해라)**
6) 기록된 이미지는 배포범위가 넓혀지지 말아야 한다 – 예를들면 언론매체나 인터넷에서 일상적으로 인식할 수 있도록 되어서는 안된다(제2, 제7, 8정보보호원칙).
7) 그 이미지를 배포범위를 넓히려 한다면 관리자 혹은 지정된 직원에 의해 결정되어야 한다. 그러한 결정의 이유가 기록되어야 한다(제7정보보호원칙).
8) 그 이미지가 언론에 공개하는 경우 그 이미지는 인식되지 않도록 가장되거나 익명처리 해야 한다(제1, 제2, 제7 정보보호원칙).
9) 그 시스템이 그러한 유형의 편집을 수행하는 설비를 가지고 있지 않다면 편집회사를 고용할 필요성이 있을 수 있다.
10) 편집회사가 고용된다면 관리자와 지정공무원은 다음과 같은 사항을 확인할 필요성이 있다.
    - **a) 정보통제자와 편집회사간의 계약관계**
    - **b) 편집회사가 그 이미지의 보안조치에 관하여 적당한 보증을 했는가**
    - **c) 그러한 보증이 지켜졌는지를 관리자는 확인해야 한다.**

***03.치안시책자료❹341~362 2005.2.23 10:29 AM 페이지346

d) 편집회사는 관리자 혹은 지정관리직원의 지시에 따라 이미지를 사용한다고 계약서에 명시했는지

e) 계약서상에 편집회사에 의해 안전보장을 한다고 기술되어 있는가 (제7 정보보호원칙)

11) 그 이미지를 받은 언론사는 편집을 한다면 제7 정보보호원칙이 적용될 것이다.

6. 정보대상자에 의한 접근

이것은 1998년 법 제7조에 규정되어 있는 권리이다. 이러한 권리에 대한 상세한 해설은 '98 정보보호법 해설 부분을 참조하면 된다. 그 기준은 다음과 같다.

1) 장비를 운영하는데 관련된 모든 직원은 정보대상자의 접근요청을 인정할 수 있어야만 한다(제6, 제7정보보호원칙).
2) 정보대상자는 기준자료요청형태에 의해 신청해야 한다.
   a) 요청된 이미지를 찾아내기 위해서 필요한 정보를 받아야 한다.
   예를들면 - 특정 개인은 장비가 설치된 지점에 방문한 때의 날짜와 시간을 제공할 수 있다.
   b) 요청한 자를 인식할 수 있는 정보를 제시받아야 한다.
   예를들면 - 장비의 사용자가 요청한 자를 알지못한다면 그 이미지를 찾아내기 위해서 그 개인의 사진을 요청할 수 있다.
   c) 요청된 이미지를 찾기 위해서 청구할 수 있는 요금을 표시해야 한다. 최대 10파운드가 탐색을 위해 청구될 수 있다.
   d) 그 신청자가 기록된 이미지를 단순히 보는 것에 만족하는지를 파악해야 한다.
   e) 필요한 요금과 정보를 받은 즉시 혹은 40일 이내에 제공될 수 있다고 고지한다.
   f) 1998년법에 의한 권리를 설명한다.
3) 신청자는 기록 · 보관되는 이미지의 처리방법을 기술한 리플렛이 제공되어야 한다. 즉 그러한 이미지가 기록되고 유지되는 목적, 그러한 이미지와 관련한 공개정책에 관한 정보(제6정보보호원칙). 자세한 내용은 대상자의 권리에 대한 부분을 참고하면 된다.
4) 이러한 것들은 접근신청기준이 신청자에게 제공될 때 이루어져야 한다(제6 정보보호원칙). 자세한 내용은 대상자의 권리부분을 참고하면 된다.
5) 모든 대상자의 자료접근신청은 관리자 혹은 지정된 직원에 의해 처리되어야 한다.
6) 관리자 혹은 지정된 직원은 요청된 이미지를 찾아야 한다.
7) 관리자 혹은 지정된 직원은 개인에 대한 공개가 제3자에 대한 공개를 야기하는 것인지를 결정해야 한다(제6 정보보호원칙). 자세한 내용은 대상자권리에 대한 부분을 참고하면 됨.
8) 관리자 혹은 지정된 직원은 제3자의 이미지를 보호할 의무가 있는지를 확인할 필요가 있다(제1, 제5 정보보호원칙). 자세한 내용은 대상자의 권리부분 참조.
   예를들면 - 도시중심부 혹은 거리에서 있을 때 촬영된 개인은 외과병원 대기실에서 기다릴 때와 같은 사적공간에서 기록된 이미지보다 프라이버시 보호가 더 필요한 것은 아니다.
9) 제3자의 이미지가 공개되지 않으려면 관리자 혹은 지정된 직원은 제3자이미지가 위장되거나 익명처리될 수 있도록 조정해야 한다(제6정보보호원칙).
10) 그 시스템이 그러한 유형의 편집을 수행할 수 있는 설비를 가지고 있지 않다면 제3자 혹은 회사를 고용할 수 있다.
11) 제3자가 고용되었다면 관리자 혹은 지정된 직원은 다음을 확인해야 한다.
    a) 정보통제자와 제3자 혹은 회사사이의 계약관계
    b) 제3자 혹은 회사가 그 이미지에 관련하여 보안조치에 관하여 보증을 했는지
    c) 그러한 보증이 적당하게 충족되었는지를 관리자는 통제해야 한다.
    d) 제3자 혹은 회사가 관리자 혹은 지정된 직원의 지시에 따라 이미지를 사용해야 함을 명백히 했는지 계약서를 검토해야 한다.
    e) 계약서는 제3자 혹은 회사가 명백히 보안보증을 해야 한다.
12) 관리자와 지정된 직원은 대상자인 개인의 접근신청에 동의할 수 없다면 다음과 같은 사항이 기록되어야 한다.
    a) 신청을 한 개인의 신원확인
    b) 신청한 날짜
    c) 신청한 이미지제공을 거부한 이유
    d) 그 결정을 한 관리자 혹은 지정된 직원의 이름과 서명
13) 모든 직원들은 이러한 관리원칙부분에서의 개인의 권리를 숙지하고 있어야 한다(제7 정보보호원칙).

7. 다른 권리들

1998년법 제10, 12, 13조에 의한 다른 권리들은 이 원칙의 98정보보호법해설 부분에 기술되어 있다. 이 원칙의 기준은 아래와 같다.

1) CCTV장비운영에 관련된 모든 직원들은 다음과 같은 개인으로부터의 신청을 인정할 수

***03.치안시책자료❹341~362 2005.2.23 10:29 AM 페이지348

있어야만 한다.

a) 개인에게 손해를 야기할 것 같은 처리의 방지. 법 제10조는 개인은 손해와 고통을 야기할 것 같은 처리를 방지하는 권리를 가지고 있다. 자세한 내용은 다른 권리에 대한 부분참조.

b) 그러한 개인과 관련하여 자동적인 결정의 방지. 그러한 시스템의 사용자들은 자동적 의사결정에 관련하여 개인의 권리에 관한 법 12조의 효과를 알아야 한다.

2) 모든 직원들은 그러한 신청에 책임있는 관리자 혹은 지정직원을 알고 있어야 한다.

3) 실질적이고 보호받지 못하는 손해를 야기할 것 같은 처리를 방지하기 위한 신청과 관련하여 관리자 혹은 지정직원은 신청자들이 동의하는지 혹은 동의하지 않는지를 표시해야 한다. 법 제10조는 개인에게 실질적인 손해 혹은 고통을 야기할 것 같은 처리를 방지할 권리를 부여한다.

4) 관리자 혹은 지정직원은 결정을 요구하는 신청을 받았을 경우 21일 이내에 개인에게 문서로 답변해야 한다. 법 10조는 개인에게 실질적인 손해 혹은 낙담을 야기할 것 같은 처리를 방지할 권리를 부여한다.

5) 관리자 혹은 지정직원은 그 신청이 인정될 수 없다고 결정한 경우 개인에게 그 이유를 소명해야 한다. 법 10조에 따라 개인은 실질적인 손해 혹은 낙담을 야기할 수 있는 처리를 방지할 권리를 가지고 있다.

6) 신청서류, 답변서류의 복사본이 보관되어야 한다.

7) CCTV시스템에 의한 자동적인 결정(automated decision)이 개인에게 내려졌다면 관리자와 지정직원은 그러한 결정을 개인에게 통지해야 한다. 그러한 시스템의 사용자들은 1998년법 제12조의 효과를 알아야만 한다.

8) 그러한 통지에 있어서 21일이내에 개인이 문서로 번복을 요청할 경우에는 관리자 혹은 지정직원은 시스템에 의한 자동적인 결정을 재고해야 한다. 그러한 시스템의 사용자들은 1998년법 제12조를 정확히 알고 있어야 한다.

9) 자동화된 결정에 대해 재고요청을 받은 경우에 관리자와 지정직원은 21일이내에 개인의 요청에 동의한다는 단계를 수립해야 할 것이다.

10) 관리자 혹은 지정직원은 다음의 사항을 기록해야 할 것이다.

a) 원래의 결정

b) 개인으로부터의 신청

c) 개인으로부터의 신청에 대한 답변

8. 법규준수여부의 감독

1) 계약내용은 근무시간동안 시민들이 열람할 수 있어야 한다. 계약사항을 기획하는 종업원들은 이러한 장비사용의 정책과 절차를 알아야 한다.

2) 신청이 있는 경우 신청자에게 다음과 같은 것들이 제공되어야 한다.

a) 접근신청을 받은 경우 그 개인에게 소책자(leaflet)배부

b) 관련서류의 복사본

c) 신청을 받은 경우의 접근신청양식

d) 개인이 그 시스템의 사용에 대해 동의하는 경우 준수해야 하는 이의신청절차

e) 이러한 원칙조항에 동의하지 않는 경우 준수해야 하는 이의신청절차

3) 이의신청절차는 명확하게 기록되어야 한다.

4) 이의신청한 건수와 성질에 대한 기록은 처리한 조치와 함께 보관되어야 한다.

5) 관리자와 지정직원은 공공의 반응과 여론을 평가하기 위해서 이의신청건수에 대한 보고서를 작성 · 수집해야 한다.

6) 관리자와 지정직원은 관련규정이 준수되고 있는지를 확인하기 위해서 장부들을 정기적으로 검토해야 한다.

7) 법적 규제와 원칙에 대한 준수여부가 지켜지고 있는지 감시할 수 있도록 이러한 검토 보고서가 정보통제자에게 제공되어야 한다.

8) 그 시스템의 효과성을 평가하는 1년단위의 내부평가가 실행되어야 한다.

9) 그 보고서의 결과는 그 계획의 목적에 따라 평가되어야 한다. 그 계획이 그러한 목적을 성취하는 것이 아니라면 중지되거나 변경되어야 한다.

10) 그러한 보고서의 결과는 공표되어야 한다.

***03.치안시책자료❹341~362 2005.2.23 10:29 AM 페이지350

Ⅲ. '98 情報保護法(The Data Protection Act 1998) 解說

1. 정의

CCTV 시스템 혹은 이와 유사한 감시장비의 사용자들이 1998년법의 요건을 준수하는지를 결정하기 위해서 고려해야 하는 용어의 정의가 있다. 이것은 법 제 1, 2조의 내용이다.

a) 정보통제자(data controller)

"개인정보가 처리되는 혹은 처리되어야 하는 목적과 방법을 결정하는 자(홀로 혹은 다른 사람과 공동으로)". 예를들면 범죄를 예방과 탐지, 범죄자의 체포와 기소, 공공안전의 보호 등의 목적으로 도시중심지에 CCTV를 설치하기 위해서 협력하는 경찰과 지역당국이 있다면 그들 둘은 모두 이러한 목적을 위한 정보통제자들이다.

예를들면 경찰, 지방자치단체, 지역상인이 범죄의 예방과 탐지, 범죄자의 체포와 기소, 공공안전의 보호를 목적으로 도시중심부 혹은 쇼핑센타에 CCTV를 설치하기로 결정했다면 위의 모든 당사자는 이 계획을 수행할 목적의 정보통제자이다. 그리고 그들은 이미지를 사용하기 위해서 정책을 세워야 한다(규정의 기준부분에서 요약했듯이).

정보통제자들은 관리자에게 일상적 운영권을 위탁할 수 있으나 관리자가 정보통제자가 되는 것은 아니다. 그는 정보통제자의 지시와 정보통제자가 설정한 정책에 따라 그 계획을 관리할 수 있을 뿐이다.

그 계획의 관리자가 정보통제자들의 고용인이라면 그 관리자는 정보통제자의 역할인 자료보호책임을 수행해야 하는 것은 아니다. 그러나 관리자가 이미지의 획득및 배포와 관련하여 정보통제자들의 지시이외의 조치를 취한다면 그는 고용계약을 위반할 뿐만이 아니라 1998년법 제55조를 위반한 것이다. 관리자가 정보통제자에 의해 고용된 시큐리티회사같은 제3자라면 그 관리자는 정보처리자(data processor)로 간주될 수 있다. 이는 정보통제자를 위해 개인정보를 처리하는 사람인 것이다. 정보통제자가 정보처리자를 고용하기로 했다면 제7 정보보호원칙에 부합되어야 한다.

b) 개인정보(personal data)

개인관련 정보: 현재하는 정보, 소유하거나 소유할 예정인 정보, 정보통제자로부터의 정보. 1998년 법은 유럽규약(European Directive)에 바탕을 둔 것이다. 그 유럽규약의 내용(European

Directive 95/46/EC)은 개인정보의 처리에 있어서의 개인보호와 그러한 정보의 자유운동에 관한 것이다.

1998년법 제2조는 사적 정보를 다음과 같이 정의한다. 개인정보는 개인을 특정할 수 있거나 특정하여 식별할 수 있는 정보를 의미한다. 특정하여 식별될 수 있는 이란 직접적으로 혹은 간접적으로 식별번호 혹은 신체적, 생리적, 정신적, 경제적, 문화적, 사회적으로 특정될 수 있는 요소에 관한 것이다. 개인정보의 정의는 정보통제자가 특정한 이미지에 이름을 붙일 수 있는 경우에 한정되지 않는다. 구별가능한 개인의 특징에 관한 이미지가 처리되고, 그 개인이 그러한 이미지로부터 식별될 수 있다면 이러한 것들은 모두 개인정보에 해당한다.

c) 민감한 개인정보(sensitive personal data)

1998년법 제2조는 민감한 사적 정보를 구분해 놓고 있다. CCTV운영규정에서 가장 중요한 목록은 제2조의 내용이다. 이 부분은 CCTV사용자들과 관련된 목록의 몇가지를 언급한다.

- 어떤 범죄의 위반 혹은 추정된 위반
- 위반 혹은 추정된 위반 혹은 범법에 대한 소송, 소송절차 혹은 그러한 소송에서의 법원의 선고

후자는 상인들이 지역경찰과 연합하여 CCTV를 설치한 경우 특히 중요할 것이다. 그리고 경찰은 상가에서 다발하는 절도를 방지하기 위한 목적으로 촬영된 이미지와 경찰이 보유한 경력범죄자 정보를 비교하여 범법자들을 식별할 수 있는 용도로 사용한다.

정보통제자가 민감한 개인정보를 처리할 것인가 혹은 처리하지 않을 것인가를 결정하는 것은 중요하다. 왜냐하면 제1의 정보보호원칙에 따라 동의를 받아야 하는 것 때문이다.

d) 처리(processing)

1998법 제1조는 처리할 수 있는 유형을 열거하고 있다. "정보 혹은 데이터와 관련하여 수집, 처리, 기록, 보관, 운영이란 정보 혹은 데이터의 조직, 적응, 변경, 수선, 상담, 사용, 공표 · 배포, 조정, 조합, 지우기, 파괴 등을 포함한다". 이러한 정의는 다른 별도의 규정이 필요없을 정도로 이미지를 기록하고 보관하는 과정을 포괄적으로 적용할 수 있다. 또한 이미지의 실시간 전달을 적용할 수도 있다. 그리하여 카메라 앞을 지나가는 개인의 이미지는 모니터에 실시간으로 나타난다면 이것은 전달, 배포, 혹은 다른 사람들이 볼 수 있는 것으로 구성된다.

따라서 이미지의 정밀한 포착과 사용에 있어서 어떠한 경우에도 1998년법의 처리에 대한 정의이내에서 대처할 수 있다.

***03.치안시책자료❹341~362 2005.2.2310:29AM 페이지352

2. 개인정보와 이미지가 처리되는 목적

정보보호원칙에 따라 동의를 구하기 전에 감시장비와 CCTV사용자들은 다음의 두가지 문제를 결정하는 것이 필요하다.

- 어떠한 유형의 개인정보가 처리되고 있는가는 1998년 법 제2조에서 정의한 민감한 개인정보의 정의이내에서 찾아야 한다.
- 개인정보와 민감한 개인정보가 어떠한 목적으로 처리되는가?

감시장비의 사용자들은 관련장비에 포착된 정보와 이미지를 사용하려는 목적을 명확히 해야한다. 그러한 장비는 다음과 같은 목적으로 사용될 수 있다.

- 범죄의 예방, 수사, 탐지
- 범법자의 체포와 소추(형사소추 증거인 이미지를 포함하여)
- 공공과 종업원의 안전
- 교통흐름의 모니터링

감시시스템에 의해 촬영된 정보의 경우 사적 정보 혹은 민감한 사적 정보와 마찬가지로 반드시 엄격한 기준에 의해 처리되어야 하는 것은 아니다. 예를들면 교통혼잡에 대한 최신정보를 시민들에게 제공하기 위해서 교통흐름을 모니터링하는 시스템은 반드시 사적정보의 처리기준을 따라야 하는 것은 아니다.

3. 정보보호원칙

1) 제1 정보보호원칙

개인정보는 공정하고 합법적으로 처리되어야 할 것이다. 특히 법 제2조의 조건 중의 하나가 최소한 충족되지 않는다면 처리하지 말아야 한다. 민감한 개인정보의 경우에 최소한 법 제3조의 조건중의 하나를 충족해야 한다. 이러한 원칙이 지켜졌는지를 진단하기 위해서 정보통제자는 다음과 같은 문제를 고려해야 한다.

a) 개인정보 혹은 민감한 개인정보가 처리되는가?

법 제2조에 민감한 개인정보에 대한 정의는 상세하게 기술되어 있다. 특히 CCTV 관련부분은 CCTV 사용자들에게 관련성이 높은 목록들을 언급하고 있다. 법2조의 민감한 정보에 대한 정의는 위에서 상술하였고, 그리고 정보통제자는 정보와 이미지를 처리하는 결정을 내릴 때 그러한 정보와 이미지의 처리가 합법적인 바탕이 있는지를 결정하기 위해서 그 조항의 목록을 참조해야 한다.

b) 처리를 위한 조건이 충족되는가?

제1의 정보보호원칙은 자료통제자가 처리에 있어서 합법성을 가졌는가를 요건으로 한다. 정보통제자는 이러한 관점에서 뒷받침되는 근거를 명확히 해두어야 한다. 이러한 것들은 그 법의 제2, 3조에 설정되어 있다. 도시중심부와 같은 공공이 출입하는 공간을 감시하는 계획의 운영자들은 제2조의 5항(d)에 따라야 한다. 왜냐하면 공공의 이익이 관련되어 있으므로 공공성이 준수될 수 있어야 하기 때문이다. 이것은 범죄의 예방과 탐지, 범법자의 체포와 소추 혹은 시민과 종업원의 안전같은 목적을 포함할 수 있다. 가게와 소매센터를 감시하는 계획의 운영자들은 제2조의 6항(1)에 따라야 한다. 정보의 처리는 합법성이 필요하기 때문이다. 다만 예외적으로 정보 대상자의 권리, 자유, 합법성이라는 이유로 공개되지 않을 수 있다. 이러한 기준이 각 개별적인 경우에 처리의 일반적 근거를 제공할 수 있음에 반하여 정보통제자의 관심 즉 감시장비의 사용자는 개인의 권리를 침해할 수 없다.

정보통제자가 민감한 개인정보를 처리하기로 결정했다면 법 제3조에 위반하지 않고 합법적이었는지를 결정할 필요가 있을 것이다. 도시중심부의 감시장비 사용자들 특히 지방자치단체 혹은 경찰(혹은 둘의 협력)의 공동으로 협력하는 경우 정보통제자들은 제7조 (1) (b)의 규정을 숙지해야 한다. 왜냐하면 법에 의해 정해지거나 관계자에게 부여된 기능을 실행하는 것이 필요하기 때문이다. 1998년 범죄와 무질서법에 위반되지 않도록 공공기관에 의한 정보와 이미지의 사용은 법정기준을 충족해야 한다.

가게 혹은 소매센터에서 기록된 정보와 이미지의 사용자들은 1998년법의 제3조(10)에 규정에 따라야 한다.

정보보호(민감한 개인적 정보의 처리) 명령 2000(S.I No 417).

예를들면-

"(1) 처리는:

a) 실질적인 공공의 관심안에 있어야 한다.

b) 불법적 행위의 예방과 탐지를 목적으로 한다.

c) 이러한 목적에서 벗어나지 않은 경우 자료대상자의 동의없이도 수행할 수 있어야 한다."

***03.치안시책자료❹341~362 2005.2.2310:29AM 페이지354

정보통제자는 정보의 처리가 합법적인 근거를 가지고 있는지 확인해야 하고, 그러한 사실을 반드시 알고 있어야 한다:
- 어떠한 정보가 처리되고 있는가
- 처리되는 이유

c) 정보와 이미지가 합법적으로 처리되는가?

합법적인 처리근거를 가지고 있다는 사실이 제1의 정보보호원칙이 충족되었다는 것을 의미하지는 않는다. 정보통제자는 그들이 처리하는 정보와 이미지가 일반법의 신뢰의 의무와 같은 법적 의무 혹은 책임이 있는지를 고려해야 한다. 공공부분은 그러한 자료의 처리에 있어서 제한 혹은 금지가 있는지를 결정하기 위해서 행정법상의 권한을 검토할 필요가 있을 것이다. 그들은 또한 1998 인간권리법의 관련성을 검토할 필요가 있을 것이다.

d) 정보와 이미지가 공정하게 처리되는가?

정보통제자가 정보와 이미지를 처리할 합법적인 근거를 가지고 있다는 사실만으로 제1의 자료보호원칙을 준수했다고 볼 수 없다.

1998법의 제1조 2 (1) - (4)의 해석조항은 공정하게 처리하기 위해서 필요한 것을 규정하고 있다. 공정하게 처리하기 위해서 최소한 다음의 정보는 이미지를 획득하는 시점에서 개인에게 제공되어야 한다.
- 정보통제자의 신원
- 정보통제자가 그 법의 목적에 따라 지정한 대표자의 신원
- 정보가 처리되는 목적
- 정보가 처리되거나 처리되어야 하는 특정환경에 관한 것 혹은 개인의 관점에서 공정하게 처리될 수 있도록 하는데 필요한 정보

e) 계약조건에 위배될 수 있는 환경

이 법은 사적 정보를 비밀리에 처리하는 것에 대해 특정한 규정을 두고 있지 않지만 공정한 처리라는 조건으로부터 제한적으로 인정된다. 공정한 처리란 개인이 그들의 이미지가 촬영될 수 있는 지역을 알고서 출입했다는 것을 인지하고 있어야 함이 필요하기 때문에 비밀적 처리 즉 촬영사실을 표시하지 않거나 제거하는 것은 제1의 정보보호원칙의 공정성을 위반한 것이다. 그러나 이러한 조건의 위반은 면책될 수 있다. 그러한 면책은 법

제29조에서 발견될 수 있다.

(1) 제29조: 다음의 목적으로 처리되는 개인정보

a) 범죄의 예방 혹은 탐지

b) 범법자의 체포 혹은 소추

a), b)의 목적은 제1첫 번째 보호원칙으로부터 면제된다(스케줄 2, 3의 조건에 따라야 하는 범위를 제외하고) ...

이것은 자료통제자가 면제되는 것으로 나열된 목적 중의 하나 혹은 두가지 모두를 위해서 이미지를 처리한다면 제1 정보보호원칙의 공정성 항목을 위반하지 않고 이미지를 획득하거나 처리할 수 있다는 것을 의미한다.

2) 제2 정보보호원칙

"개인정보는 합법적이고 특정한 목적으로만 수집되고, 그러한 목적과 부합되지 않는 목적으로 처리되지 말아야 한다" 정보통제자는 이러한 정보보호원칙을 준수했는지를 확인하기 위해서 이미지의 처리목적을 명확히 해야 한다.

특정한 목적이란 Commissioner 혹은 개인에게 통지한 것들일 수 있다.

합법성을 검토할 때에 고려되어야 하는 많은 문제들이 있다.
- 정보통제자가 처리에 대한 합법성을 가지고 있는지(제1 정보보호원칙)
- 이미지가 신뢰보호의 법적 의무, 공공부분에 대한 행정법 등의 법적 의무에 따라 처리되었는가

적합성의 원칙(requirement of compatibility)은 제3자에게 공개하려고 할 때 혹은 제3자에게 공개하려는 정책을 수립할 때 특히 중요하게 적용되는 해석조항이다.

예를 들면 이미지 처리의 목적이
- 범죄의 예방 혹은 탐지
- 범법자의 체포 혹은 소추라면

정보통제자는 적합성에 따라 정보의 공개를 원하고 있는 제3자에게 공개할 수 있을 뿐이다. 예를들면 범죄활동에 대한 수사인 경우 범법자 혹은 피해자 혹은 목격자를 인식하는데 시민으로부터 도움을 받기 위해서 언론에 범죄활동 장면을 공개하는 것은 적합한 것이다. 그러나 범죄예방과 탐지를 위해서 설치된 장비로부터의 이미지가 단지 오락적 목적으로 공개된다면 이것은 부적합한 용도일 것이다. 예를들면 반사회적 행위에 대하여 싸우는 경찰의 공권력의 적정한 사용을 보여주기 위해서 토요일 밤에 도시중심부에서 술취한 사람의 이미지를 언론에 공표하는 것은 적정할 수 있다. 그러나 오락적인 목적으로 이와같은 이미지가 언론에 제공된다면

***03.치안시책자료❹341~362 2005.2.2310:29AM 페이지356

적합하지 않은 것일 수 있다.

정보통제자가 이미지를 처리하는 목적에 적합하여 공개하기로 결정하였다면 그 공개의 범위는 숙고할 필요가 있다. 공개되는 장면이 관련이 없는 제3자의 이미지를 포함하고 있을 경우 정보통제자는 그러한 이미지가 확인될 수 없도록 화면처리를 했는가를 확인할 필요가 있을 것이다.

정보통제자가 그러한 편집을 할 수 있는 설비를 가지고 있지 않다면 이미지의 익명처리를 조건으로 언론매체의 배포에 동의할 수 있다. 이것은 제한적으로 정보를 처리해야 함을 의미할 것이다. 그러한 경우에 정보통제자는 언론매체가 제7 정보보호원칙을 준수했는가를 확인할 필요가 있다.

3) 제3 자료보호원칙

"개인정보는 처리되는 목적에 충분하고 적합해야 하고, 그 목적을 넘어서서는 안된다".

설치된 목적에 따라 필요한 것 이상의 정보를 기록하지 않도록 카메라의 상황을 고려해야 함을 의미한다. 예를들면 주차장에서 자동차파괴행위를 기록하기 위한 카메라는 개인의 주거상황을 촬영해서는 안된다. 게다가 테이프에 기록된 이미지가 명확하지 않다면 그 자료는 불충분한 정보라는 것은 당연하다. 예를들면 그 시스템의 목적이 범죄활동의 증거를 수집하는 것이라면 불명확한 이미지는 합법적인 증거로 제시될 수 없을 것이고, 범죄예방이라는 목적에도 불충분할 수 있다.

4) 제4 정보보호원칙

"개인정보는 정확해야하고 필요하다면 최신으로 갱신되어야 한다".

이 원칙은 기록과 저장되는 사적 정보는 정확해야 함을 의미한다. 이것은 시스템으로부터 수집된 개인정보가 범죄행위 혹은 종업원과의 분쟁에서 증거로 사용되려면 특히 중요하다. 정보를 기록하기 위해서 양질의 테이프를 사용하는 것, 기존의 이미지를 단순히 기록하는 것이 아니라 재사용에 앞서 테이프를 깨끗이 하는 것, 과사용으로 저질화되는 것을 피하기 위해서 정기적으로 테이프를 교환하는 것 같이 이미지의 선명도를 유지하기 위해서 노력해야 함을 Commissioner는 권장하고 있다.

정보통제자의 시스템이 시간과 장소에 따라 사용될 수 있는 특징을 가지고 있다면 이러한 것들은 정확해야 한다. 그러한 특징의 정확성을 보증하는 기록절차를 유지하고 있는지 점검하고, 필요하다면 수정하고 변경해야함을 의미한다.

테이프로부터 증거로 사용되는 정지화면을 만들기 위해서 디지털기술 및 압축기술을 사용할

때에는 주의해야 한다. 가끔 이러한 기술은 선행의 프로그램 장면이 남아 있을 수 있기 때문이다. 그리하여 사용자들은 그 테이프로부터 얻은 이미지가 실제장면을 정확하게 묘사하고 있는지를 확인할 수 없다. 이것은 법원 혹은 내부직원 징계청문회 등에서 사용하는 것이라면 증거로 사용하기 어려울 수 있다.

5) 제5 정보보호원칙

"특정한 목적하에 촬영되는 개인정보는 그러한 목적에 필요한 기간이상으로 장기간 보관되어서는 안된다".

이 원칙은 사용되는 목적에 필요한 기간을 초과하여 보관되지 말아야 한다는 것을 지적하고 있다. 관련활동을 기록한 테이프는 관련 절차가 완성되고, 이의제기의 가능성이 없을 때까지 보관되어야 한다. 그러한 기간이 경과된 때에는 폐기되어야 한다. 이러한 조건에 위배하여 저장 · 기록한 이미지는 부당한 기간동안 보관되지 말아야 한다. 이미지의 보관기간에 대한 정책은 정보의 특징, 수집되는 목적을 고려하여 수립되어야 한다. 예를들면 쇼핑지역의 범죄예방을 위하여 이미지가 기록되는 곳에서 보관되어야 하는 유일한 이미지는 특정의 범죄활동에 관련된 것이다. 나머지는 곧 폐기될 수 있다. Commissioner는 도시중심부계획의 이미지가 증거로 사용될 것이 아니라면 28일을 초과하여 기록된 이미지를 보관하지 말아야 한다고 지적하고 있다.

6) 제6 정보보호원칙

"개인정보는 법률에 따라 자료대상자의 권리에 부응하여 처리되어야 한다"

법률은 개인정보의 처리에 관련하여 많은 권리를 개인에게 제공한다... 다음의 권리를 위반하는 것은 제6 정보보호원칙을 위반하는 것이 된다.

- 개인은 관련 정보를 복사하여 제공받을 개인의 권리
- 손해와 고통을 야기하는 처리를 방지할 권리

  법 제2조는 민감한 사적 정보목록을 나열하고 있다. 이 원칙의 이러한 부분은 단지 목록의 몇가지 만을 언급한다. 그것은 CCTV 사용자에 관련된 것이다. 모든 목록을 알려면 법령의 관련부분을 참조해라.
- 자동적 결정에 관련된 권리

  시스템의 사용자들은 자동적 의사결정에 관련된 개인의 권리에 관한 1998년법의 제12조의 효과를 알아야 한다.

***03.치안시책자료❹341~362 2005.2.2310:29AM 페이지358

7) 제7 정보보호원칙

영국기준기관(British Standard Institute)-BS 7958: 1991 "CCTV관리와 운영원칙(Closed Circuit Television - Management and Operation Code of Practice)"은 보안과 테이프관리 등에 관한 안내를 제공한다.

"개인정보가 권한이 없거나 불법적인 처리, 개인정보의 우연적 손실, 파괴 혹은 훼손을 방지하기 위해서 적당한 기술적 · 조직적 조치가 취해져야 한다"

보안수준을 평가하기 위해서 정보통제자는 이러한 원칙의 준수여부를 확인해야 할 필요가 있다. 정보통제자는 다음을 평가해야 한다.

- 권한이 없거나 개인정보의 불법적인 처리, 우연적 손실, 파괴, 훼손 등으로부터 발생할 수 있는 손해

  이러한 원칙의 위반은 계획하는 목적에 악영향을 초래한다는 것을 명확히 하면서 증거나 이미지는 법정에서 사용될 수 없고, 시민들도 부적당한 공개 때문에 감시장비의 사용에 신뢰가 무너질 수 있다. 법률에 의한 손해검토는 촬영된 사람들에 대한 영향을 검토해야 한다.

- 정보의 특징이 고려되어야 한다.

  민감한 개인정보는 앞부분에서 정의되어 있으나 고려해야 할 다른 사항이 있을 수 있다. 예를들면 도시중심부 계획은 주차된 차안에서 키스하는 커플의 이미지를 동시에 촬영 기록할 수 있고, 상인들의 계획은 옷을 갈아입는 탈의실에서 대상자의 이미지를 기록할 수 있다(의류의 도난을 방지하기 위해서). 이러한 이미지들은 제2조에서 열거한 목록이 아니지만 그러한 이미지가 촬영된 사람들에 대한 정보는 고려되어야 하고, 신중하게 처리되어야 한다는 것은 명확하다.

8) 제8 정보보호원칙

"개인정보는 사적 자료의 처리에 관하여 자료대상자의 권리와 자유를 충분하게 보호하지 않는 EEA(European Economic Area) 외부의 국가나 지역에 유포하면 안된다".

이 원칙은 EEA외부의 국가나 지역에 사적 정보를 배포하는 것에 제한을 두고 있다. 정보통제자가 사적 정보를 해외에 유포하기를 원할 것 같지는 않지만 정보통제자는 인터넷 혹은 웹사이트에 게시하지 말아야 한다. 이러한 원칙이 위반되지 않도록 정보통제자는 1998년법의 제4조를 고려해야 한다.

4. 촬영기록된 대상자의 접근권리

정보통제자에게 서면요청을 하고 수수료를 지불하는 즉시 개인은 다음과 같은 권리가 있다.

- 누가 개인정보를 촬영했는 지를 고지받을 권리
- 촬영되었다면 촬영된 개인정보, 촬영되는 목적, 열람할 수 있는 사람들
- 알수 있는 방법으로 고지받을 권리

a) 모든 개인정보

이러한 정보는 복사본의 형태로 제공되어야 한다. 그러한 복사본의 제공이 가능하지 않거나 개인이 다른 방법을 원한 경우를 제외하고 복사본의 형태로 제공되어야 한다. 복사된 정보가 구체적 설명없이는 이해할 수 없다면 개인은 그러한 정보에 대해서 설명을 받아야 한다. 그 때에 정보통제자는 촬영된 정보가 기록된 테이프를 Code에 대한 암호없이는 이해할 수 없는 형태로 정보를 보관한다.

b) 정보의 소재와 알아볼 수 있는 방법에 관한 정보

정보통제자는 그러한 정보가 어디에 있는지 혹은 어떻게 인식될 수 있는지에 대한 정보를 알려줄 의무는 없다. 정보통제자는 대상자의 열람에 대해서 수수료를 청구할 수 있다. 정보통제자는 열람청구를 한 40일이내에 신청에 동의해야 한다.

- 자료를 찾는 데 필요한 정보(신청을 한 사람의 인적사항과 신청자의 요구정보)
- 수수료

정보통제자가 문서로 신청하고 소정의 수수료를 납부하지 않았다면 정보통제자는 그 요청에 동의할 필요가 없다. 정보통제자가 대상자로부터 소정의 수수료 혹은 그 대상자의 신상정보를 받지 않았다면 그 신청에 대해 40일이내에 신청에 대한 답변을 하기 위해서 수수료납부와 개인정보를 요청해야 한다. 동일한 사람이 동일한 혹은 비슷한 재신청을 한 경우 과거의 요청과 현재의 요청사이에 합리적인 기간이 경과하지 않았다면 그 요청에 동의할 필요가 없다. 합리적인 간격이라는 것이 어떤것인가 결정하는데 있어서 다음과 같은 요인들이 고려되어야 한다: 정보의 특성, 정보처리의 목적, 정보가 수정되는 빈도.

대상자의 접근요청에 대한 대응으로서 제공하는 정보는 신청서에 기재된 개인의 모든 정보를 포함해야 한다. 그러나 자료의 일상적인 수정과 삭제는 요청된 날짜와 답변의 날짜사이에 계속되어야 한다. 이러한 범위에서 개인에게 제공한 정보는 요청을 받은 때의 정보와 개인의 정보와 차이가 있을 수 있다. 심지어는 그 정보가 더 이상 보관되지 않는 수도 있다. 그러나 신청을 받으면 정보통제자는 특별한 수정 혹은 삭제를 하지 말아야 한다. 그 정보는 개인이

***03.치안시책자료❹341~362 2005.2.23 10:29 AM 페이지360

받아들일 수 있도록 수정되지 말아야 한다.

대상자의 신청에 동의하여 열람하기로 한 경우 대상자 이외의 다른 사람과 관련된 정보가 공개될 수 있는 경우에 정보통제자는 특별히 고려해야 하는 문제가 있다. 법률은 이러한 문제를 인정하고, 그러한 환경에서 대상자의 신청에 동의할 의무가 있는 정보통제자가 지켜야 할 두 개의 경우를 규정한다.

- 다른 사람이 그 정보의 공개에 동의한 경우
- 다른 사람의 동의 없이 신청에 동의하는 것이 합리적인 경우

그 법은 관련된 다른 개인의 동의없이 요청에 응하는 것이 합리적인가를 해석하는데 도움을 준다. 이러한 문제를 결정하는데 있어서 주의해야 하는 것들은 특히 다음과 같다.

- 다른 사람에 대한 비밀의 의무
- 다른 사람의 동의를 얻을 목적으로 정보통제자가 취한 조치
- 다른 사람이 동의가능한 가에 대한 것
- 다른 사람의 동의거부 표현

신청자가 그 정보로부터 다른 개인이 누구인지를 알 수 없다면 정보통제자는 그 정보를 제공해야 한다.

정보통제자가 그 법을 위반하여 대상자의 접근요청에 동의하지 않는다면 신청대상자는 자료통제자가 그 요청에 동의하지 않는다는 명목으로 법원에 소송을 제기할 수 있다. 정보통제자가 법에 위반하여 동의하지 않은 것으로 법원이 인정하면 그에 따라 정보통제자는 열람신청을 받아주어야 한다고 법원으로부터 명령을 받을 수 있다.

5. 촬영된 대상자의 자료접근배제

개인의 접근권을 배제하는 경우가 있다. 이러한 관련 규정은 법 제29조에서 발견할 수 있다. 이 규정에 따라 대상자의 접근권이 배제된다. 이것은 제1 정보보호원칙에서 공정한 처리에서의 자료접근배제와 유사한 것이다. 범죄예방과 탐지, 범법자의 체포와 소추를 목적으로 개인정보가 보관되는 경우 정보통제자는 대상자의 접근요청을 거부할 권한이 있음을 의미한다. 제1 정보보호원칙의 공정하게 처리해야 한다는 원칙이 배제되는 것과 같이 접근요청에 대한 거부권한은 케이스 바이 케이스로 구체적 사건에 따라 판단되어야 한다.

6. 그 밖의 권리

1) 손해 혹은 고통을 야기하는 정보처리의 방지권

법 제10조에 따라 개인은 개인정보를 처리함에 있어서 시작하거나 중지하도록 정보통제자에게 통지할 권리를 가지고 있다. 문제가 되는 처리가 실질적으로 개인과 다른 사람에게 손해 혹은 고통을 야기한다는 이유로 그러한 통지를 할 수 있을 뿐이다. 어떤 경우에는 이러한 통지가 적용되지 않는 경우도 있다. 이 경우는 개인이 동의한 경우이다; 대상자와의 계약과 관련된 경우, 정보통제자의 법적 의무가 있는 경우, 개인의 치명적인 이익을 보호하기 위한 경우이다. 정보통제자가 그러한 통지를 받은 경우 그러한 통지에 동의한다든지 정당하지 않다든지를 21일이내에 답변해야 한다.

2) 자동적 결정(Automated Decision-Taking)과 관련된 권리

그 법의 제12조에 따라 개인은 그들에게 중요한 영향을 미치는 경우에 자동적인 결정을 방지할 권리를 가진다. 이 규정은 개인에 대한 업무평가와 그들의 책임소재와 같은 문제의 결정을 고려한 것이다. 이것은 개인이 계약과정에서 동의한 것이며, 이러한 자동적 결정을 법규화한 것이다. 이 법은 기계적 수단에 의한 정보처리를 인정하는 것이며, 개인과의 계약과정에서 동의한 것이다. 기계적 결정은 법규에 의해 권한이 부여된 것이고, 개인의 합법적인 이익을 보호하기 위한 것이다. 집행되기 전에 그 결정에 대해 변명하도록 허용하는 것과 같은 문제를 포함할 수 있다.

개인의 이의제기가 없더라도 개인에게 중요한 영향을 미치는 자동적 처리에 있어서 정보통제자는 그 결정이 자동적 처리에 의해서 취해진 것이라고 통지할 의무가 있다. 개인은 그러한 통지를 받은 21일이내에 그러한 결정에 재검토하고, 새로운 결정을 바란다고 정보통제자에게 요구할 수 있다. 그러한 통지를 받은 경우 정보통제자는 21이내에 답변을 해야 한다.

이러한 상황은 CCTV감시의 경우에 자동적 안면인식과 같은 자동의사결정기법이 활용되는 경우이다. 그러므로 이 자동의사결정은 개인의 권리를 보호하기 위해 심사숙고하는 것은 중요하다. 특히 촬영된 개인에게 어떠한 조치를 취해야 하는가에 대한 결정은 기계적인 촬영뿐만이 아니라 인간의 개입이 있어야 한다면 자동적 처리에만 의존해서는 안된다.

자동적인 의사결정에 있어서 개인의 이의신청이 받아들여지지 않는다면 개인은 권리를 보호하기 위해 법원에 소송을 제기할 수 있다.

***03.치안시책자료❹341~362 2005.2.23 10:29 AM 페이지362

3) 특정요구조건에 동의하지 않은 경우의 배상

제13조를 위반한 결과로 손해 혹은 고통을 받은 개인은 법원에 손해배상소송을 제기할 권리가 있다. 이러한 소송제기와 함께 Data Protection Commissioner에게 법률을 준수하였는지 위반하였는지에 관한 판단을 요청할 권리가 있다.