

개인정보의 공개와 보호에 관한 연구*

- 영국 사례를 중심으로 -

김 정 애**

1. 머리말
2. 영국 정보공개법의 주요내용과 개인정보 관련 규정
 - 1) 정보공개법 일반
 - 2) 비공개대상정보
 - 3) 개인정보 관련 규정
3. 영국 데이터보호법의 주요내용과 개인정보 관련 규정
 - 1) 데이터보호법 일반
 - 2) 비공개대상정보
4. 개인정보의 접근을 위한 정보공개법과 데이터보호법
 - 1) 정보공개법과 데이터보호법의 개인정보조항에 관한 법률적 상호관계
 - 2) 정보공개법과 데이터보호법의 개인정보조항 비교·분석
5. 맺음말

* 본 논문은 김정애의 경북대학교 석사학위논문(2008)에서 요약한 것으로 2011년 한국기록학회 월례발표회 발표문을 수정·보완한 것입니다.

** 논산시 지방기록연구사

[국문초록]

정보화 사회에서 정보는 개인 뿐 아니라 단체, 기업, 구각 등의 조직에 있어서도 중요한 자원으로 인식된다. 국가적인 차원에서 국민들에게 가능한 많은 정보를 공개하고 이용할 수 있도록 하는 동시에 개인정보를 보호하거나 비밀을 유지하는 등의 프라이버시와 관련된 권리 역시 보호하고 있다. 기록학에서는 이러한 문제를 ‘접근(access)’이라는 개념으로 다루고 있다.

공공기관이 보유한 정보를 최대한 공개하는 것이 정보공개법의 원칙이고, 개인정보 처리과정에서 다루어지는 개인정보를 최대한 보호하는 것이 데이터보호법의 원칙이다. 이처럼 두 법률이 지향하는 바는 정보의 최대 공개와 최대 보호라는 점에 차이가 있다. 그러나 국민의 알 권리를 충족시키기 위해 정보를 최대한 공개하는 동시에, 프라이버시 권리의 보장을 위해 정보를 최대한 보호하기 위해서는 두 법률이 적절한 균형을 이룰 필요가 있다.

영국은 공공기관의 정보공개를 위한 일반법으로 정보공개법(Freedom of Information Act 2000)을, 개인정보보호를 위한 일반법으로 데이터보호법(Data Protection Act 1998)을 제정했다. 데이터보호법은 1984년에 제정되어 시행되다 1995년 유럽연합(European Union, EU) 개인정보보호지침의 요구에 부합하기 위해 1998년에 개정되어 오늘날까지 개정 법률을 적용하고 있다. 정보공개법은 미국, 유럽의 다른 나라에 비해 비교적 늦게 제정되었는데 토니 블레어 총리 내각이 열린 정부(Open Government) 정책을 추구하면서 2000년에 정보공개법이 제정되었고 2005년에 시행되었다. 정보공개법이 시행되면서 기존의 기록물관리법에 규정된 접근 조항을 폐지하고 정보공개법에 통합시켰다.

이 연구는 영국의 사례를 중심으로 개인정보 관련 조항을 검

토하고 두 법률이 상호보완적으로 작용하는 부분과 상충하는 부분을 연구하고자 한다. 이를 바탕으로 공공기관의 개인정보를 처리하는 과정에서 두 법률 사이의 적절한 균형을 이루는 방법을 밝히고자 한다.

주제어: 개인정보, 알 권리, 프라이버시권, 정보공개법, 개인정보보호법

1. 머리말

지식정보화사회가 도래하면서 정보는 개인 뿐 아니라 단체, 기업, 국가 등의 조직에 있어서도 중요한 자원으로 인식된다. 양질의 정보를 얼마만큼 보유하고 있는가는 정보사회에서 앞설 수 있는 중요한 요소이며 경쟁력이다.

정보를 점차 중요한 자원으로 인식함에 따라 이를 둘러싼 여러 가지 문제들이 야기되기 시작했다. 매일 대량으로 쏟아지는 정보 속에서 양질의 것을 선별하는 정보의 질적인 측면에 대한 문제에서부터, 정보통신기기 등 제반여건의 미비로 인해 정보에 균등하게 접근할 수 없는 분배의 불균형 문제, 대중매체로부터 일방적으로 정보를 수용하던 입장에서 벗어나 다양한 통로를 통해 다각적으로 정보에 접근할 수 있게 되면서 정보의 수정·침해·왜곡 문제가 발생한다.

이러한 상황은 단지 개인적인 차원에서의 문제로 그치는 것이 아니라 국가적인 차원에서도 다루어지게 되었다. 오늘날 행정조직의 기능이 비대해지고 복잡해지면서 공공기관에서는 국민들에게 가능한 많은 정보를 공개하고 이용할 수 있도록 하는 동시에, 정보에 포함된 개인

정보를 보호하거나, 비밀을 유지하는 등 프라이버시와 관련된 국민의 권리를 보호하기 위해 노력하고 있다.

제도적인 차원에서 국민의 알 권리를 보호하기 위해 정보공개제도를, 프라이버시권을 보호하기 위해 개인정보보호제도를 확립하여 시행하고 있다. 공공조직이 보유한 모든 정보를 최대한 공개하는 것이 정보공개법의 기본 원칙이고, 개인정보 처리과정에서 다루어지는 개인정보를 최대한 보호하는 것이 데이터보호법의 기본 원칙이다. 이처럼 두 법률이 지향하는 바는 정보의 최대 공개와 최대 보호라는 점에 차이가 있다. 두 법률이 지향하는 바는 다르지만 알 권리와 프라이버시권을 최대한 보호하기 위해서는 두 법률이 적절한 균형을 이룰 필요가 있다.

따라서 이 연구는 우리나라와 비교적 비슷한 시기에 정보공개법과 데이터보호법이 제정된 영국의 사례를 바탕으로 각 법률에 규정된 개인정보에 관련된 조항을 검토하고 두 법률이 상호 보완적으로 작용하는 부분과 상충하는 부분을 연구함으로써 두 법률 사이의 적절한 균형을 이루는 방법을 밝히고자 한다.

2. 영국 정보공개법의 주요내용과 개인정보 관련 규정

1) 정보공개법 일반

영국의 정보공개제도는 유럽의회, 유럽연합 등 범유럽 지역기구의 정보공개, 열람, 접근에 대한 규범에서 영향을 받아 만들어졌다. 다른 나라에 비해 비교적 늦게 제도가 확립되었는데 2000년 법률이 제정되고 2005년에 본격적으로 시행되었다. 시행까지 5년이란 시간이 걸린

것은 영국정부가 ‘안전보장 예비단서’로 5년을 제시했기 때문이다. 즉 5년 동안은 법 시행을 위한 준비단계로 설정해 법률의 효과적인 시행을 준비하고, 발생할 수 있는 문제에 대처할 수 있도록 여러 가지 준비과정을 거쳤다. 이 법이 시행되면서 1958년과 1967년 공공기록물법 (Public Records Acts)에 있는 접근 조항은 폐지되었다.

이 법에 따라 공공기관은 모든 기록을 공개해야 한다는 원칙에 따라 기록에 대한 접근을 정당화했다. 이것은 정보접근에 대한 관점을 바꾸었고 기록관리 전반에 걸친 시스템에도 변화를 초래했다. 확실하고 정확한 기록의 생산·관리·보존이 이루어져야 행정의 투명성이 제고되고 신뢰받는 정보공개도 이루어질 수 있기 때문이다.

제도의 원활한 시행을 위해서 정보공개법이 시행되기 전인 2002년부터 각 공공기관은 효율적인 법률의 시행을 위해서 정보공개목록 (Publication Schemes)을 의무적으로 작성했다. 정보공개법 제19조에 공공기관의 정보공개목록 작성을 의무화하고 있다. 영국 정보공개법의 일반적인 사항은 아래 <표 1>과 같다.

<표 1> 정보공개법의 일반적인 사항

항 목	내 용
개인정보의 범위	신원확인이 가능한 생존하는 개인에 관한 정보
정보공개청구권자	영국 국민과 영구 내 혹은 외국에 거주하는 외국인도 가능
대상기관	공공기관 ¹⁾
접근권	공공기관에서 보유하고 있는 기록된 제3자의 정보
개인정보 형태	<ul style="list-style-type: none"> · 컴퓨터로 작성된 문서 · 컴퓨터나 CCTV같은 장치로 처리된 정보 · 의료, 사회복지사업 관련 기록과 지방자치단체의 주택이나 학교의 학생과 관련된 기록 · 정렬되어 구조화된 수기 기록 · 공공기관에서 보유하고 있는 모든 형태의 수기기록에

		포함된 정보
절차상의 측면	청구형식	특정한 형식 없음 (서면이나 이메일로 신청)
	수수료	열람 청구의 범위에 따라 결정
	청구인 제시정보	이름, 주소, 청구정보에 대한 세부사항, 청구정보의 공개 형태(필요한 경우) 등
	공공기관의 답변기간	해당정보 보유여부 통지, 접수일로부터 20일 이내
청구거절 (비공개)		<ul style="list-style-type: none"> · 동일 청구인이 이미 공개된 정보 혹은 동일한 정보에 대해 여러번 청구한 경우 · 수수료 규정을 초과할 경우(중앙기관은 £ 600, 그 외 기관은 £ 450) · 제40조 비공개조항에 해당하는 경우
이의제기		<ul style="list-style-type: none"> · 공공기관에 내부심사 요구 · 재검토가 거절되면 정보감독관에 불복구제심사 제기 · 정보감독관의 판결에 만족하지 않는다면 정보심판위원회에 상소 · 정보감독관을 거치지 않고 바로 법원에 소송 제기 가능

정보가 비공개대상정보 조항에 해당되거나 비공개하는 것이 공공의 이익을 위해 더 가치 있는 경우를 제외하고는 공공기관은 공개청구된 정보를 의무적으로 제공해야 한다.

영국에서는 독립적인 위치에서 정보공개제도를 감독·심판·집행·조정하는 기구로 정보감독관을 두고 있다. 정보감독관은 여왕이 임명하는 독립기관으로 정보감독관의 결정은 법원과 정보심판위원회의 감시를 받는다. 정보감독관의 결정은 법적인 구속력을 갖는 것은 아니지만 대부분 공공기관에서 정보감독관의 방침과 결정을 수용하기 때문에 중요한 의미를 가진다.

정보감독관은 영국 내에서 정보공개법이 올바르게 시행되도록 공공

1) 이 법의 적용대상기관은 중앙행정기관과 지방자치단체, 국회, 국방부, 의료기관, 초·중·고등학교, 종합대와 단과대를 포함한 대학교 등의 교육기관, 국경기관, 잉글랜드, 웨일즈, 북아일랜드에 위치한 공기업 등 (스코틀랜드는 자체 정보공개법을 보유하고 독자적으로 법을 적용하고 있다)

기관의 정보공개법 시행을 감독·평가·조정하고 필요한 조언을 제공한다. 또한 정보공개 교육과 훈련을 담당하고 실제로 공공기관에서 개인정보 공개업무를 수행할 때 참고할 수 있는 여러 가지 지침을 발행한다. 그리고 개인정보를 보유하거나 이용하는 개인이나 기관은 정보의 내용과 이용목적 등을 서면으로 정보감독관에 미리 신고해야 하며, 정보감독관에 등록하지 않은 개인정보는 공개하거나 이용할 수 없다.²⁾

2) 비공개대상정보

모든 기록을 공개한다는 정보공개법의 기치 아래 30년이 경과되지 않은 비공개 기록도 공개하기 시작했다. 또한 기록관리기관에서 이관받아 공개한 30년이 경과한 영구보존기록에 비공개를 적용한 경우도 대부분 해제되었다.

비공개조항은 다시 완전면제(absolute exemption)와 조건부면제(qualified exemption), 제한면제(more limited class exemption)로 구분할 수 있다. 완전면제에 해당하는 비공개조항³⁾은 국민의 알 권리가 적용되지 않기 때문에 공익검증심사(Public Interest Test) 대상이 될 수 없다. 따라서 해당 정보를 공개할 필요가 없고, 공공기관은 해당정보의 보유 여부를 확인해줄 의무가 없다.⁴⁾

2) 최정열, 2002, <인터넷과 개인정보의 보호>, 《정보법학》 제6권 제1호, 한국정보법학회, 128쪽.

3) 제21조 청구인이 다른 수단에 의해 접근할 수 있는 정보 (TNA의 역사기록은 예외), 제23조 안보문제를 다루는 조직이 제공했거나 그 조직에 관련된 정보 (TNA의 역사기록은 예외), 제32조 법원 기록, 제34조 국회의 특권에 해당하는 정보, 제36조 하원이나 상원이 보유한 정보와 관련해 효과적인 공무 수행을 저해하는 경우, 제40조의 일부조항 개인정보, 제41조 기밀로 분류된 정보, 제44조 기타 법률이나 내규 등에 의해 공개가 제한되는 경우

4) 정부혁신지방분권위원회, 2005, 《국 거버넌스 실현을 위한 국민참여적 정보공

정보감독관은 공공기관에서 공익검증심사를 수행할 때 고려해야 하는 사항들을 제시하는데⁵⁾ 첫 번째, 정보공개청구 가능성이 있는 정보 인지를 예상하고, 두 번째, 기관 의사결정자의 의견을 수렴한 정책을 고안하는 것이다. 마지막으로 선행사례를 고려하는 것이다. 정보감독관에서 이루어진 선행사례를 통해 비슷한 유형의 청구를 어떻게 처리하는지 검토할 수 있다.

정보를 비공개하는 것이 정보의 존재 확인이나 공개보다 가치가 있을 경우, 조건부면제가 적용된다. 조건부면제의 경우⁶⁾에는 공익검증심사를 수행하여 정보를 비공개하거나 존재여부를 확인하지 않는 것이 공공의 이익에 부합한다고 판단될 경우에만, 정보를 비공개하거나 존재여부를 확인하지 않아도 된다.

제한면제는 조건부면제보다 공개제한이 더욱 엄격히 적용된다. 제한면제대상은 국방, 국제관계, 경제, 범죄예방, 상업적 이해관계에 악영향을 끼치거나, 효과적인 공무수행을 저해하는 정보이고, 이 경우에는 침해검증심사(Predjudice Test)를 수행할 의무가 있다.⁷⁾ 정보공개법에서는 공개정보에 일부 비공개항목이 포함되어 있다면, 이 부분을 제외하고 정보를 공개해야 한다고 규정하고 있다.⁸⁾ 이 규정은 전체정보를 비공개하는 것이 아니라 부분공개를 권장한다는 의미로 해석할 수 있다.

개제도 활성화 방안 연구》, 행정자치부, 47쪽.

5) ICO, Awareness Guidance No.3, pp.5~6.

6) 제22조 향후 출판될 예정인 정보, 제23조 TNA가 보관한 역사기록과 관련된 경우, 제24조 국가안보, 제26조 국방, 제27조 외교, 제28조 영국 내정, 제29조 경제, 제30조 공공기관에 의해 수행된 투자와 소송, 제31조 법률의 시행, 제33조 감사, 제35조 정부 정책의 수립, 제36조 효과적인 공무 수행을 저해하는 경우, 제37조 여왕과 고위 공직자들의 통신, 제38조 보건, 제39조 환경 정보, 제40조 일부조항 개인정보, 제42조 법률상 비밀 보호 권리, 제43조 상업적 이해

7) 정부혁신지방분권위원회, 위의 책, 44쪽.

8) Freedom of Information 2000, Part II, s29.

3) 개인정보와 관련된 규정

정보공개법에서의 개인정보(personal information)는 신원확인이 가능한 생존하는 개인에 관한 정보로 그 범주는 다음과 같다.⁹⁾

- 컴퓨터로 작성된 문서
- 컴퓨터나 CCTV와 같은 장치로 처리된 정보
- 의료, 사회복지사업 관련 기록과 지방자치단체의 주택이나 학교의 학생과 관련된 기록
- 정렬되어 구조화된 수작업으로 처리된 기록
- 공공기관에서 보유하고 있는 모든 형태의 수기 기록에 포함된 정보

마지막 항목은 ‘e범주 데이터(category e data)’라고도 하며 정보공개법에 의해 데이터보호법에 도입되었다. 민간부문의 조직에서는 구조화되지 않은 파일링시스템(filing systems)에 보유된 개인정보는 범주에 포함되지 않는다.

〈표 2〉 정보공개법 제40조 제1항~제4항

제40조(개인정보)
① 정보공개를 청구하는 데이터주체 본인의 개인정보는 공개청구대상에서 제외된다.
② 공개청구에 해당하는 정보가 다음과 같다면, 공개청구대상에서 제외된다. 1. 제1항에 포함되지 않는 개인정보로 구성되어 있고 2. 아래에 제시된 첫 번째 혹은 두 번째 조건 중 어느 하나를 만족시킨다.
③ 첫 번째 조건은 1. 1998년 데이터보호법 제1조 제1항에서 규정한 ‘데이터’의 정의에 해당하는

9) ICO, 2007, Awareness Guidance No.1, p.1.

제1호에서부터 제4호까지의 조항을 만족시키는 경우, 이 법에 의거해 일반 대중에게 정보를 공개하는 것이

가. 데이터보호원칙을 침해할 경우
 나. 데이터보호법 제10조(손실 혹은 불이익을 초래할 것 같은 정보의 처리를 막을 권리에 관한 조항)에 위배되는 경우

2. 다른 경우에, 데이터보호법의 제33조의1 제1항(공공기관에서 보유하고 있는 수작업으로 처리된 데이터에 관한 조항)에 적용된다면, 이 법에 의거해 일반 대중에게 정보를 공개하는 것은 데이터보호원칙에 위배된다.

④ 두 번째 조건은 데이터보호법 제4장 비공개대상정보조항이 적용되어 이 법 제7조 제1항 제3호에서 규정하고 있는 데이터주체접근권에서 제외되는 경우이다.

정보공개법의 개인정보조항 중 가장 중요하게 다루어야 할 부분이 비공개대상에 포함되는 조항이다. 제2장 비공개대상정보조항 중 제40조가 개인정보에 관한 내용을 다루고 있다. 제40조의 개인정보는 데이터보호법과 밀접한 관계를 가지고 있다. 또한 정보공개법의 데이터보호원칙은 데이터보호법 부칙 1의 제1장에 규정된 ‘8가지 데이터보호를 위한 원칙’을 의미한다. 데이터주체와 개인정보라는 용어 역시 데이터보호법 제1조 제1항에서 사용하는 용어와 의미가 일치한다.

정보공개법 제40조는 크게 두 가지 유형의 개인정보 비공개사항을 명시하고 있다.

1. 만일 청구정보가 데이터주체, 즉 본인의 개인정보이면 이 정보는 공개하지 않는다. (제40조 제1항)
2. 만일 청구정보가 데이터주체가 아닌 제3자의 개인정보라면, 그리고 이 정보를 공개하는 것이 데이터보호법에 저촉된다면 이 정보는 공개하지 않는다. (제40조 제2항)

데이터주체 즉, 개인정보가 본인의 정보일 경우 정보공개법 제40조 제1항에 의해 비공개조항이 된다. 대신 이 경우에는 데이터보호법의

데이터주체접근 규정에 의거해서 공개를 요청할 수 있다. 즉, 청구인 본인의 개인정보에 대한 접근은 정보공개법에 근거하지 않고 데이터보호법에 근거해 이루어진다. 청구정보가 데이터주체 본인의 정보가 아닐 경우라면, 정보공개법에 의거해 정보에 접근할 수 있는 가능성이 생긴다.

제3자의 개인정보를 공개 요청하는 경우에도 비공개한다고 규정했다. 정보공개법 제40조에서는 데이터보호법의 구체적인 조항을 명시해 데이터보호법 조항들에 어긋나면 비공개한다고 규정했다.¹⁰⁾ 즉, 제3자에 대한 정보공개를 요청할 때 공공기관은 정보공개법뿐만 아니라 데이터보호법도 고려해 비공개여부를 결정해야 한다.

구체적으로 첫째, 데이터보호법 제1조제1항제1호~제4호까지의 ‘데이터’ 정의에 해당하는 정보일 경우, 데이터보호법의 8가지 데이터보호원칙에 위배되거나, 데이터보호법 제10조¹¹⁾에 위배되면 비공개한다. 둘째, 데이터보호법 제33조제1항에 위배될 경우 공개되지 않는다. 데이터보호법 제33조 제1항은 공공기관에서 보유하고 있는 수기데이터(manual data)에 관련된 규정이다. 세 번째, 데이터보호법 비공개대상정보조항에 적용되어 동법 제7조제1항제3호에 해당하는 정보접근권리가 없는 사람에게는 정보가 비공개된다. 데이터보호법 제7조제1항제3호는 개인정보에 관한 데이터주체의 접근권을 규정하고 있다.

제40조제1항은 완전면제로 이루어져 있기 때문에 공익검증심사가 적용되지 않는다. 제40조제2항의 데이터보호법의 8가지 데이터보호원칙에 위배되는 경우 역시 완전면제이기 때문에 공익검증심사가 적용되지 않는다.

제40조제3항제1호가의 데이터보호법 제10조에 위배되는 경우는 공

10) Freedom of Information Part II s40 (2), (3), (4).

11) 데이터보호법 제10조는 데이터주체나 다른 사람에게 피해를 줄 수 있는 정보 처리를 방지할 수 있는 권리를 규정하고 있다.

익검증심사를 적용할 수 있다. 이 경우 모든 상황을 고려하여 공익을 위한 공개여부를 검토해야 한다. 또한 데이터관리자가 공개여부를 판단하는데 있어 정보를 공개하는 것이 데이터주체나 제3자에게 피해를 줄 가능성이 있다면 데이터관리자는 그 정보의 공개를 신중하게 고려해야 한다.

제40조제3항제2호의 데이터보호법 제4장비공개조항에 해당하는 경우 역시 공익검증심사의 대상이 된다. 이 경우 공공기관은 모든 상황을 검토해 공익을 위해 정보를 비공개하는 것이 더 가치가 있을 경우에만 비공개될 수 있다. 또한 데이터보호법 제4장의 데이터주체접근권에서 비공개조항으로 보호받는 공익을 확인하고 공익이 정보공개법 제40조제2항에 근거해 비공개조항으로 보호되고 있는지 필수적으로 고려해야 한다.

정보공개법 제40조에 의거해 비공개되는 정보에 동법의 다른 비공개조항이 함께 적용될 수 있다.¹²⁾ 예를 들어, 국가안보기관에서 근무한 사람의 개인정보 공개를 청구할 경우, 개인정보는 제40조를 적용할 수 있지만 그 개인정보에 국가안보에 관한 사항이 포함되어 있을 경우 정보공개법 비공개대상정보조항 제23조 ‘안보문제를 다루는 조직이 제공했거나 그 조직에 관련된 정보’를 적용할 수 있다. 그리고 제40조 비공개조항을 적용하는 것보다 제23조를 적용하는 것이 정보공개를 거부하는 공공기관의 입장에서는 훨씬 손쉽고 확실한 이유가 될 수 있다.

공공기관에서 개인정보를 공개할 때 위에서 살펴본 정보공개법의 비공개조항에 해당되지 않아 공개가 가능할 경우라도 데이터보호법에 저촉된다면 공개할 수 없다. 이 때문에 데이터보호법에서 다루고 있는 개인정보의 내용에 대해 함께 살펴봐야 하는 것이다.

12) <http://www.dca.gov.uk/foi/guidance/exguide/sec40/chap06.htm>.

3. 영국 데이터보호법의 주요내용과 개인정보 관련 규정

1) 데이터보호법 일반

1980년대 들어서 프라이버시 문제에 대한 국제적인 관심이 증대하면서 1980년 경제협력개발기구 ‘프라이버시 보호 및 개인정보의 국제적 유통에 관한 지침’과 유럽평의회(Council of Europe)의 ‘개인데이터의 자동처리에 관한 개인의 보호를 위한 유럽협약’이 제정되었다. 이 국제기구의 회원국인 영국 역시 데이터보호를 위한 국제적인 노력에 동참하여 1984년 데이터보호법을 제정했다.¹³⁾

그리고 프라이버시권 보호를 명시하고 있는 유럽연합의 95/46/EC 지침이 1995년 제정되면서 1998년 영국 역시 자국의 데이터보호법을 개정했고 2000년 3월부터 시행되었다. 데이터보호법의 일반적인 사항은 아래의 <표 3>과 같다.

<표 3> 데이터보호법의 일반적인 사항

항 목	내 용
개인정보의 범위	신원확인이 가능한 생존하는 개인에 관한 정보 ¹⁴⁾
정보공개 청구권자	데이터주체
청구대상기관	· 공공기관 · 은행, 공익사업체, 회사조직 등 민간기관
접근권	데이터주체 자신에 대한 개인정보(데이터주체접근권)
개인정보 형태	· 컴퓨터에 저장된 혹은 저장될 정보 · 컴퓨터나 CCTV 같은 장치로 처리된 정보 · 고도로 조직화된 수기 파일링시스템에 포함된 정보

13) 오항녕, <영국 정보공개제도의 발달과 현황: 미완의 여정>, 《기록보존》 제 12호, 행정자치부 국가기록원, 1999, 117쪽.

14) 원칙적으로 사망한 사람의 정보는 데이터보호법에 의해 보호받을 수 없다. 단,

		· 의료, 교육, 공공서비스 혹은 주택 관련 기록 · 공공기관에서 보유한 정보
절차상의 측면	청구형식	특정한 형식 없음 (서면이나 이메일로 신청)
	수수료	보통 £ 10 정도
	청구인 제시정보	이름, 주소, 신원확인, 청구정보에 대한 세부사항, 청구정보를 찾기 위해 필요한 다른 정보에 대한 세부사항 등
	공공기관의 답변기간	접수일로부터 40일 이내
청구거절 (비공개)		· 동일 데이터주체에 의한 동일 혹은 유사한 주체접근청구가 이미 이루어진 경우 · 데이터주체의 개인정보에 제3자의 개인정보가 포함되어 있고 제3자가 그 정보의 공개에 동의하지 않는 경우 · 제4장 비공개조항에 해당하는 경우
이의제기		· 공공기관에 내부심사 요구 · 재검토 거절 혹은 재검토 후에도 거절되면 정보감독관에 불복구제심사 제기 · 정보감독관의 판결에 만족하지 않는다면 정보심판위원회에 상소 · 정보감독관을 거치지 않고 바로 법원에 소송 제기 가능

데이터보호법에 의해 보호되는 ‘데이터’는 원칙적으로 자동처리방식으로 처리된 것, 연관파일링시스템(relevant filing system)의 일부로서 기록된 것, 이 법 제68조에서 정의한 접근 가능한 기록¹⁵⁾의 일부를 구

사망한 사람의 유전적인 정보가 그 사람의 선조와 자손 모두에 영향을 미치는 것처럼, 사망한 사람의 정보가 살아있는 사람의 개인정보에 해당하는 경우는 예외적으로 간주한다.

15) 제68조 “접근 가능한 기록”의 의미

① 데이터보호법에서 “접근 가능한 기록”의 의미는

1. 제2항에서 정의하는 의료 관련 기록
2. 부칙 11에서 정의하는 교육 관련 기록
3. 부칙 12에서 정의하는 접근 가능한 공기록

② 제1항 제1호의 “의료 관련 기록”의 의미는

1. 육체적 혹은 정신적인 건강 상태 혹은 개인의 상태와 관련된 정보로 구성된 것
2. 개인의 건강관리와 관련해 의료 전문가에 의해 작성되거나 의료 전문가를 대신해 작성된 것.

성하는 것을 의미한다.¹⁶⁾ 여기서 ‘데이터나 정보의 처리’는 ① 데이터나 정보의 조직, 응용 혹은 변경 작업, ② 데이터와 정보의 검색, 참고 혹은 이용, ③ 데이터나 정보의 전달, 보급 혹은 이용 및 공개, ④ 데이터나 정보의 정렬, 조합, 차단, 삭제 혹은 파기 등의 작업들을 의미.¹⁷⁾

1984년 데이터보호법은 자동으로 처리된 데이터에만 적용되었지만, 1998년 개정된 법에서는 95/46/EC지침에 부응하기 위해 컴퓨터로 작성·처리된 정보 외에도 수기 파일링시스템¹⁸⁾도 정보의 범주에 포함되었다.

‘데이터주체’는 이 법 제1장제1조에 의거 개인정보의 주체가 되는 개인을 의미하며 동법 제7조에 의거한 주체접근(subject access)은 데이터주체가 본인의 개인정보에 접근하는 것을 의미한다.

특히 동법 제2장제7조에 규정된 ‘주체접근권(subject access rights)’은 데이터주체가 자신의 개인정보에 대해 접근할 수 있는 권리로, 이 주체접근권에 의해 데이터주체가 자신의 개인정보를 보유한 기관이나 조직에 공개를 청구하는 것을 ‘주체접근청구(subject access requests)’라고 한다.

데이터보호법에 따라 데이터주체는 자신의 개인정보에 대해 접근할 수 있는 권리(제7조~제9조), 손해나 어려움을 야기할 정보의 처리를 저지할 권리(제10조), 직접적인 마케팅을 목적으로 자신의 정보를 직접적인 마케팅을 목적으로 사용하는 것을 저지할 권리(제11조), 자신의 개인정보에 대해 자동의사결정이 이루어지는 것에 반대할 권리(제12조), 데이터보호법을 위반하는 행위로 인해 입은 손실에 대해 보상

16) Data Protection Act 1998 Part I s1.

17) Data Protection Act 1998 Part I s1.

18) 수작업처리데이터란 연관파일링시스템의 일부로서 기록된 것이어야 한다. 연관파일링시스템이란 자동처리형식으로 수집된 정보는 아닐지라도 쉽게 접근할 수 있는 개인에 관한 특정한 정보로 개인과 관련이 있는 일련의 정보를 말한다.

받을 권리(제13조), 자신에 대한 부정확한 개인정보의 수정·차단·삭제·과기할 수 있는 권리(제14조, 제12조의1, 제62조)를 보장받는다.

‘데이터관리자’는 개인정보를 처리하는 방법과 목적을 결정하는 사람을 의미한다. 데이터관리자는 필사기록, 사업 활동 관련 핵심정보, 자선단체 회원기록 등 몇 가지 정보를 제외한 모든 개인정보의 처리에 대해 정보감독관에게 반드시 그 과정을 통보하고 등록해야 한다. 데이터관리자가 이러한 의무를 위반하여 부당하게 개인정보를 침해하는 행위를 했을 경우 민사상 손해배상 책임은 물론 형사상 제재도 받을 수 있다.¹⁹⁾ 더불어 데이터관리자는 정보처리의 목적, 청구인이 누구인지에 대한 내용을 포함하여 정보의 처리여부를 데이터주체에게 통지해야 한다.

〈표 4〉 데이터보호법 제7조 개인정보에 대한 접근권

<p>제7조(개인정보에 대한 접근권)</p> <p>① 데이터주체는 다음 권리를 가진다.</p> <ol style="list-style-type: none"> 1. 데이터관리자나 위탁인에 의하여 데이터주체의 개인정보가 처리되는 것을 데이터관리자로부터 통보 받을 권리 2. 개인정보가 처리되었다면, 데이터관리자에게 다음 기술(description) 사항을 통보받을 권리 <ol style="list-style-type: none"> 가. 데이터주체 자신의 개인정보 나. 개인정보가 처리되거나 처리될 예정인 목적 다. 개인정보를 공개 요청한 수령인 3. 알기 쉬운 형태로 데이터주체에게 다음 사항을 통보할 권리 <ol style="list-style-type: none"> 가. 데이터주체 자신의 데이터를 구성하는 정보 나. 그 데이터의 출처에 대해 데이터관리자가 습득하고 있는 정보 4. 데이터주체에게 심각한 영향을 끼치는 데이터주체의 업무수행도, 신용도, 책임성, 행동 등에 대한 평가가 개인정보의 자동화처리의 유일한 근거가 되는 경우, 자신에게 영향을 끼치는 의사결정논리를 데이터관리자로부터

19) ICO, Data Protection Act 1998 Legal Guidance, pp.16~17.

통보 받을 권리

- ② 데이터관리자가 다음 사항을 받지 않았다면, 데이터관리자는 제1항에 명시된 정보를 데이터주체에게 제공할 의무가 없다.
 - 1. 서면으로 된 청구
 - 2. 규정된 최대 금액을 초과한 수수료
- ③ 데이터관리자가 데이터주체의 신원을 확인하고, 공개청구정보의 위치를 찾는데 필요한 정보를 제공받지 않았다면, 데이터관리자는 데이터주체의 청구를 따를 의무가 없다.
- ④ 신원을 확인할 수 있는 정보가 포함된 공개청구를 데이터관리자가 수행하지 않아도 된다면 데이터관리자는 다음의 경우에 공개청구를 수행하지 않아도 된다.
 - 1. 제3자가 자신의 개인정보 공개에 동의하지 않은 경우
 - 2. 제3자의 동의 없이 정보를 공개하는 것이 모든 상황을 고려했을 때 합법적이지 않은 경우
- ⑤ 제4항에서 제3자의 정보를 참조하는 것은 공개청구의 출처로서 신원을 확인할 수 있는 개인정보를 참조하는 것을 포함한다. 이 세부조항은 공개청구정보에 관련된 제3자의 이름을 생략하거나 다른 신원확인 사항을 비공개하고 데이터관리자가 통보하지 않아도 된다는 뜻은 아니다.
- ⑥ 제4항 제2호의 규정에 의해 제3자의 동의 없이 정보를 공개하는 것이 모든 상황을 고려했을 때 합법적인지 결정하기 위해 다음 사항을 고려해야 한다.
 - 1. 제3자에게 지워진 기밀의무
 - 2. 제3자의 동의를 얻기 위해 데이터관리자가 실행한 절차
 - 3. 제3자가 동의할 수 있는지의 가능성 여부
 - 4. 제3자의 동의 거부 표현
- ⑦ 이 조항에 따라 개인정보를 공개 청구한 사람은 자신의 청구가, 규정된 기술 사항(description)에 대한 개인정보에 제한된다는 것을 명시한다.
- ⑧ 제4항을 수행하기 위해, 데이터관리자는 제7조에 따라 즉시 공개청구를 처리해야 하고, 공개청구의 처리는 법률에 규정된 시기가 끝나기 전에 이루어져야 한다.
- ⑨ 제7조의 조항들에 의거한 데이터주체의 공개청구를 공공기관이 부당하게 거부했다는 특정인의 주장을 법원이 인정한다면, 법원은 데이터관리자에게 공개청구를 처리해야 한다고 판결할 것이다.

데이터보호법에는 8가지 데이터보호원칙이 수록되어 있다. 데이터관리자는 비공개대상정보조항이 적용되는 경우를 제외하고는 이 8가지 데이터보호원칙에 따라서 데이터를 처리해야 한다.²⁰⁾

1. 개인정보는 공정하고 합법적으로 처리되어야 한다.
 - 특히 부칙 2에 규정된 조건들을 최소한 하나라도 충족시키지 않는다면
 - 그리고 민감한 개인정보의 경우에 부칙 3에 규정된 조건들 가운데 최소한 하나라도 충족시키지 않는다면 처리되어서는 안 된다.
2. 개인정보는 오직 하나 혹은 그 이상의 특수하고 합법적인 목적을 위해서만 취득되어야 하고, 그 목적과 모순된 방식으로 처리되어서는 안 된다.
3. 개인정보의 관리는 정보가 처리되는 하나 이상의 목적과 관련해서 이루어져야 하고 목적에 어긋나서는 안 된다.
4. 개인정보는 정확해야 하고, 필요한 경우에는 가장 최신의 상태로 유지되어야 한다.
5. 특정 목적을 위해 처리되는 개인정보는 그 목적이 필요한 기간보다 오래 유지되어서는 안 된다.
6. 개인정보는 데이터보호법에 명시된 데이터주체의 권리에 따라 처리되어야 한다.
7. 개인정보의 불법적인 처리와 개인정보의 우연한 소실·파기·훼손에 대해 적절한 조치가 취해져야 한다.
8. 유럽경제공동체 역외에 있는 국가나 지역이 데이터주체의 권리와 자유를 충분히 보호하지 않는 한, 개인정보를 그 국가나 지역으로 전송해서는 안 된다.²¹⁾

20) Data Protection Act 1998 Part I of the Schedule1.

21) 제8원칙은 95/46/EC 지침 제25조를 적용하여 만들어진 것으로, 데이터보호법 부칙1 제2장 제13조에 명시된 충분한 수준 보호란 개인정보의 성질, 정보의 발신국이나 발신지, 정보의 최종 착신국이나 착신지, 데이터처리의 목적과 처리기간, 해당 국가나 지역에서 효력을 가지는 법률, 그 국가나 지역의 국제적 의무, 그 국가나 지역에서 효력을 지니고 있는 행위규범이나 기타 지침, 그 국가나 지역에서 해당 데이터에 취해지는 안전보호조치 등을 고려할 때 적절하다고 인정되는 것을 의미한다.

8가지 데이터보호원칙 중에서 정보공개법과 직접적으로 관련된 것이 바로 제2원칙과 제5원칙이다.²²⁾ 조사·연구를 목적으로 개인정보를 이용할 경우 이 두 가지 원칙에 의거하여 공개여부를 판단해야 하기 때문이다.

이 두 가지 원칙과 함께 데이터보호법 제4장제33조 역시 정보공개법과 밀접한 관계가 있는 ‘연구·역사·통계 예외사항’을 규정하고 있다.²³⁾ 구체적인 내용은 개인정보를 무기한 보존할 수 있고 다음 두 가지 조건을 갖추면 연구 목적으로 정보를 제공할 수 있다는 것이다. 첫째, 특정인과 관련된 우호적인 추측이나 판단을 위해 데이터를 가공·처리하지 않고, 둘째, 데이터주체에 실질적인 손해나 손실을 유발할 수 있는 데이터를 가공하지 않는다는 것이다. 이러한 조건을 충족시킨다면 제3자 역시 연구목적으로 기록관리기관에서 개인정보에 대해 접근할 수 있다. 물론 이 경우 역시 정보제공기관은 정보감독관에게 연구목적으로 데이터에 접근할 의도라는 것을 공지해야 한다.

데이터주체접근청구에 의해 데이터주체가 자신의 개인정보 공개를 요청할 때 해당정보에 제3자의 정보가 포함되어 있을 수 있다. 이 경우 제3자의 동의가 없다면 정보를 공개할 수 없다고 명시하고 있다.

동법 제7조제4항과 관련된 규정에서 정보를 공개할 때 가장 명확하게 해야 할 부분은 제3자의 동의를 얻었는가 하는 것이다. 제3자에게 동의를 얻었다면, 데이터관리자는 제3자와 관련된 정보를 공개할 수 있다. 그러나 데이터관리자가 동의를 얻어야 할 의무는 법에 규정되어 있지 않다. 실제로도 제3자의 동의를 구하는 것은 어려운 일인데, 제3자를 찾는 것도 어려울 뿐 더러 찾았다 할지라도 제3자가 동의를 하지 않을 수 있고 동의를 구하는데 많은 노력이 수반될 수 있다. 이러한

22) Elizabeth Shepherd and Geoffrey Yeo, “Managing Records: A Handbook of Principles and Practice, London: Facet Publishing”, 2003, p.127.

23) Data Protection Act 1998 PartIV s33.

경우에는 이 법 제7조제4항제2호에 명시되어 있는 제3자의 동의 없이 정보를 제공하는 것이 모든 상황을 고려했을 때 타당하다고 판단되면 정보를 공개할 수 있다.

만일 제3자의 정보가 공개를 청구한 데이터주체에게 이미 제공된 적이 있거나 일반적으로 대중들이 이용하는 것이 가능하다면, 이런 정보에 대해서는 데이터관리자가 쉽게 정보의 공개를 결정할 수 있다.

데이터관리자가 제3자의 동의를 얻지 못했거나, 제3자의 동의 없이 정보를 제공하는 것이 모든 상황을 고려했을 때 불합리하다고 판단되면 데이터관리자는 그 정보를 공개해서는 안 된다. 그러나 이런 정보를 공개하는 최상의 방법은 최대한 정보를 공개하되 제3자와 관련된 부분을 변경하거나 삭제하는 것이다.

2) 비공개대상정보

예외적인 상황에서는 데이터주체의 권리가 적용되지 않을 수 있는데, 데이터보호법 제4장의 비공개대상정보조항에서 그 구체적인 조항을 다음과 같이 규정하고 있다.

- 제28조 국가안보
- 제29조 범죄와 과세
- 제30조 의료, 교육, 사회사업
- 제31조 규제행위
- 제32조 출판, 문학, 예술
- 제33조 연구, 역사, 통계
- 제34조 법률에 의해 대중이 이용할 수 있는 정보
- 제35조 법에 의한 혹은 법적인 절차에 관련된 정보공개
- 제36조 개인의 가정사와 관련된 목적
- 제37조 그 외의 부수적인 사항들

제38조 명령에 의해 비공개를 인정하는 권한
제39조 과도기적인 구제

이들 비공개조항은 데이터보호법 전체에 적용되는 것이 아니기 때문에 각 조항은 제한적이고 다양한 규정에 의해 비공개된다. 그 예로 제34조는 데이터관리자가 법령에 근거하여 공개된 정보라면, 데이터주체접근규정을 통한 개인정보에의 접근은 이루어지지 않는다는 것을 규정하고 있다. 제37조에 있는 ‘그 외의 부수적인 사항’의 자세한 내용은 동법 부칙 7에 명시되어 있다. 부칙 7의 첫 번째 항목에서도 데이터주체접근규정에 의해 개인정보를 비공개하는데, 기관에서 고용 등을 목적으로 취득된 비밀문의사항으로 개인정보가 이루어진 경우가 해당한다.

4. 개인정보접근을 위한 정보공개법과 데이터보호법

1) 정보공개법과 데이터보호법의 개인정보조항에 관한 법률적 상호관계

정보공개법과 데이터보호법의 개인정보조항에 관한 법률적 상호관계를 알아보기 위해 크게 청구인이 데이터주체인 경우와 청구정보가 제3자와 관련된 경우로 나누어 검토하도록 한다.

(1) 청구인 본인과 관련된 정보공개청구

공개청구대상정보가 청구인 자신에 관한 정보라면, 그 정보는 정보공개법 제40조제1항에 의해 비공개되며 대신 데이터보호법 제7조 주

체접근청구에 따라 공개가 이루어진다.

데이터보호법에 의해 청구할 수 있는 개인정보의 형태는 컴퓨터에 저장된 정보, 고도로 조직화된 수기 파일링시스템에 있는 정보, 의료·교육·공공서비스 혹은 주택 관련 기록, 공공기관에서 보유한 다른 정보 등을 들 수 있다. 1998년 데이터보호법은 1984년 데이터보호법에 비해 개인정보 형태의 범위를 넓혀서 조직화된 수기 파일링시스템도 개인정보의 정의에 포함시켰다.

청구정보가 청구인 개인의 정보로만 구성된 경우는 드물다. 대다수가 청구인 개인정보와 함께 제3자의 정보도 포함된다. 이 경우 처리과정은 크게 두 가지로 나누어 볼 수 있다.²⁴⁾

첫 번째로 정보 전체가 청구인 개인정보와 제3자의 정보를 모두 포함하고 있는 경우이다. 실제 청구의 대다수가 이에 해당한다. 이 경우 데이터주체의 정보와 제3자의 정보에 해당하는 내용을 분리해서 적용해야 한다. 예를 들어 청구인이 공공기관에 자신의 가족과 관련된 기록을 청구했을 때, 이 정보에는 청구인의 정보와 함께 제3자인 가족구성원의 정보도 포함된다. 청구인 본인의 정보는 데이터주체접근청구에 의한 공개여부와 절차를 따라야 한다. 그러나 다른 가족 구성원들의 정보는 제3자의 정보에 대한 공개여부와 절차에 맞추어서 검토되어야 한다.

두 번째로 청구정보 중에서 단 하나의 정보만이 청구인 개인과 제3자에 관련된 내용일 경우이다. 예를 들어서 ‘A’라는 사람이 청구인에 대해 표현한 의견이 정보에 포함되어 있다면, 이것은 청구인의 정보와 제3자인 ‘A’의 정보가 모두 포함되어 있는 것이다. 이런 경우에는 청구인 본인에 관한 정보는 데이터보호법의 데이터주체청구에 의해 공개여부와 그 절차가 검토되어야 한다.

24) <http://www.dca.gov.uk/foi/guidance/exguide/sec40/chap02.htm>.

(2) 제3자와 관련된 정보공개청구

제3자와 관련된 정보에 대해서는 비공개하는 사항에 초점을 두고 검토하도록 한다. 정보공개법 제40조 제2항, 제3항, 제4항에 제3자의 개인정보가 비공개되는 사항을 다루고 있으며 정보공개법에서는 데이터보호법에 근거해 제3자와 관련된 개인정보를 비공개한다. 구체적인 내용은 세 가지로 나누어 검토하고 더불어 공인인 제3자의 개인정보 공개에 대한 문제도 살펴보고자 한다.

1. 데이터보호원칙에 위배되는 경우
2. 데이터보호법 제10조에 위배되는 경우
3. 데이터보호법 제4장 비공개대상정보조항에 해당하는 경우

① 데이터보호원칙에 위배되는 경우

데이터보호법의 8가지 데이터보호원칙은 공공기관에서 개인정보 처리시 준수해야 할 사항들이다. 제3자의 정보를 공개하는 것이 데이터보호원칙에 어긋난다면 그 정보는 정보공개법 제40조제3항제1호에 의해 비공개된다. 8가지 데이터보호원칙을 침해하지 않는 경우에 한해서 개인정보가 공개되어야 한다. 그 중에서 정보공개와 가장 밀접하게 관련된 것이 제1원칙이다.

개인정보는 공정하고 합법적으로 처리되어야 하며, 특히 부칙 2에 규정된 조건들 가운데 최소한 하나라도 충족시키지 않는다면 그리고 민감한 개인정보의 경우에 부칙 3에 규정된 조건들 가운데 최소한 하나라도 충족시키지 않는다면 처리되어서는 안 된다.

개인정보는 합법적으로 처리되어야 한다. 정보가 합법적으로 처리되지 않으면 데이터보호원칙 제1원칙을 침해하게 되고 그 정보는 정보공개법 제40조제2항에 근거해 비공개된다. 개인정보처리가 법률적인 규정을 침해한다면 제1원칙에 위배된다. 예를 들면, 정보의 공개가 인권법(Human Rights Act 1998)이나 환경정보규정에 위배된다면 그 정보의 처리는 불법이다. 또한 공공기관이 정보를 공개할 권한이 없다면 그 정보의 공개는 불법적인 것이다. 공공기관의 정보공개 권한여부는 정보공개법과 관련된 것이 아니라 그 기관의 권한과 관련된 문제이다. 공공기관은 우선 기관이 국민에게 합법적으로 정보를 공개할 수 있는지를 자문해야 한다. 공공기관이 정보공개를 할 권한을 갖고 있지 않다면 정보는 정보공개법 제40조 제2항에 의해 공개되지 않는다.

그리고 제1원칙에는 개인정보를 공정하게 처리해야 한다고 명시되어 있다. 공정함은 합법성에 비해 그 개념이 구체적이지 않고 불명확하다. 개인정보의 공정한 처리를 위해선 공개 요청의 목적 뿐만 아니라 정보를 입수한 방법도 중요하게 고려해야 한다.

또한 정보공개는 청구인의 신원확인과 청구 목적을 파악함으로써 공정하게 이루어질 수 있다. 공공기관은 특정인이 아닌 일반 대중에게 정보를 공개하는 것이 불공평한 것인지 아닌지를 고려해야 한다. 그리하여 일반대중에게 정보를 공개하는 것이 불공평하다고 판단되면 그 정보는 비공개되어야 할 것이다.

〈표 5〉 데이터보호법의 부칙 2와 부칙 3

부칙 2

- 제1조 데이터주체가 정보처리에 동의한다.
 제2조 아래 목적에 따른 정보처리는 필수적이다.
 1. 데이터주체가 당사자인 계약을 이행하기 위해
 2. 계약을 맺기 위한 데이터주체청구를 진행하기 위해
 제3조 정보처리는 계약에 대한 의무가 아니라 데이터관리자가 주체인 법적 의

무를 위해 필수적이다.

제4조 정보처리는 데이터주체의 중대한 이익을 보호하기 위해 필수적이다.

제5조 아래 목적에 따른 정보처리는 필수적이다.

1. 재판의 처리를 위해
2. 특정 법률에 의거해 특정인에게 주어진 직무를 수행하기 위해
3. 여왕, 각료 혹은 정부기관의 기능을 실행하기 위해
4. 특정인에 의해 공익에 영향을 끼치는 공공성을 달성하기 위해

제6조 ① 정보의 처리는 정보를 공개하는 데이터관리자나 한 명 이상의 제3자에 의해 실행되는 합법적인 이익을 목적으로 하는 경우 필수적으로 이루어져야 한다. 단, 데이터주체의 합법적인 이익, 권리와 자유를 침해하는 이유로 처리가 정당하지 않은 경우는 제외된다.

② 국무장관의 명령에 의해 이 조건들이 충족되거나, 충족되지 않는 특별한 조건이 명확히 제시될 것이다.

부칙 3

제1조 데이터주체는 개인정보의 처리에 대해 명백히 동의한다.

제2조 ① 정보처리는 법률에 의해 임명된 데이터관리자에게 부여된 특정한 권리의 행사와 의무의 수행을 위해 필수적이다.

② 국무장관의 명령에 의해 다음의 사항이 실행될 것이다.

가. 명시된 다음의 경우에 제1항을 적용하지 않는다.

나. 명시된 더 많은 조건들 역시 충족되지 않으면 제1항의 조건이 충족되지 않는 것으로 규정한다.

제3조 아래 목적에 따른 정보처리는 필수적이다.

1. 데이터주체 혹은 다른 사람의 중대한 이익을 보호하기 위해

가. 데이터주체에 의하거나, 데이터주체를 대신한 동의가 이루어지지 않는 경우

나. 데이터관리자가 합법적으로 데이터주체의 동의를 얻을 수 없는 경우

2. 데이터주체에 의하거나, 데이터주체를 대신해 이루어진 동의가 비합법적으로 분류되는 경우 타인의 중대한 이익을 보호하기 위해

제4조 정보처리는

1. 다음 조직 혹은 협회가 이행하는 합법적인 활동일 경우 처리된다.

가. 비영리 목적으로 설립되거나 운영되는 협회

나. 정치적, 철학적, 종교적 목적 혹은 직종별 노동조합 목적으로 존재하는 협회

2. 데이터주체의 권리와 자유를 위한 적절한 보호수단과 함께 처리된다.

3. 위의 조직 혹은 협회의 회원이거나 처리목적과 관련해 합법적으로 접근할 수 있는 개인과 관련이 있다.

4. 데이터주체의 동의가 없는 개인정보를 제3자에게 공개하는 것은 포함하지 않는다.

제5조 데이터주체에 의해 계획적으로 이루어진 청구절차의 결과로서 개인정보가 공표된다.

제6조 정보처리는

1. (장차 이루어질 법적 소송절차를 포함해) 법적 소송절차를 위해 필수적이다.

2. 법적 자문을 구하기 위해 필수적이다.

3. 법적 권리들을 확립하고, 실행하거나 옹호하기 위해 필수적이다.

제7조 ① 아래 목적에 따른 정보처리는 필수적이다.

1. 재판의 처리를 위해

2. 특정 법률에 의거해 특정 개인에게 주어진 직무를 수행하기 위해

3. 여왕, 각료 혹은 정부기관의 기능을 실행하기 위해

② 국무장관의 명령에 의해 다음 사항이 실행되어질 것이다.

가. 명시된 다음의 경우에 제1항을 적용하지 않는다.

나. 명시된 더 많은 조건들 역시 충족되지 않으면 제1항의 조건이 충족되지 않는 것으로 규정한다.

제8조 ① 정보처리는 의료목적에 위해 필수적이고 다음과 같은 사람들에 의해 처리의무가 이루어진다.

1. 의료 전문가

2. 의료정보의 비밀을 누설하지 않는 의료전문가와 같이 동등한 비밀의무를 지닌 사람

② 제8조의 “의료목적”은 예방용 약품, 의료진단, 의료연구, 의료간호와 치료법 규정과 의료관리 서비스 취급에 대한 목적을 포함한다.

제9조 ① 정보처리는

1. 인종 혹은 민족에 대한 정보로 이루어진 민감한 개인정보이다.

2. 다른 인종 혹은 민족인 사람들 사이의 기회 혹은 대우(treatment)에 대한 평등유무(有無)의 검토 하에, 이러한 평등성을 촉진하거나 유지할 목적으로, 확인하거나 유지하기 위해 필수적이다.

3. 데이터주체의 권리와 자유를 위한 적절한 보호수단과 함께 처리된다.

② 국무장관의 명령에 의해 제1항 제3호에 따라 이루어지는 제1항 제1호와 제2호에 포함되는 혹은 포함되지 않는 처리에 대한 특별한 조건이 명시될 것이다.

제10조 개인정보는 제10조의 목적을 위해 국무장관의 명령에 명시된 조건으로 처리된다.

개인정보가 공정하게 처리되는 조건 중 청구정보가 데이터보호법 부칙 2의 여섯 가지 조건과 부칙 3의 열 가지 조건을 하나라도 충족하지 않는다면 그 정보공개는 자동적으로 데이터보호원칙 제1원칙을 침해하는 것이 된다. 부칙 2는 제1원칙의 목적과 관련된 조건으로 개인정보의 처리 사항을 담고 있다. 부칙 3은 좀 더 민감한 개인정보의 처리 사항을 담고 있다.

부칙 2 중 6번째 항목은 합법적이고 정당한 이익을 위해 이루어지는 정보처리에 필요한 필수조건을 명시하고 있다. 이 때 어떤 경우이든 데이터주체의 권리, 자유, 정당한 이익에 대한 침해 때문에 정보가 부당하게 처리되는 것은 제외된다.

그러나 데이터보호법 부칙 2와 부칙 3에 제시된 것은 최소한의 요구조건이기 때문에 이 조건을 충족시킨다고 하더라도 정보 처리가 불공평해질 수 있으며 데이터보호원칙 제1원칙을 침해할 수 있다.

② 데이터보호법 제10조에 위배되는 경우

청구정보가 데이터보호법 제10조에 위배되는 경우에도 정보공개법 제40조제2항에 의거한 비공개 사유가 된다. 데이터보호법 제10조는 데이터주체에게 ‘손실이나 손해를 초래할 수 있는 정보의 처리를 막을 수 있는 권리’를 부여한다. 데이터주체는 특정목적을 위한, 특정방법을 통한 개인정보의 처리가 자기 자신이나 다른 사람에게 실질적인 손실이나 불이익을 초래할 경우에 데이터보호법 제10조에 근거해 데이터관리자에게 개인정보의 처리를 중지하거나 시작하지 않도록 요청하는 통지를 보낼 수 있다. 제10조에서는 이를 ‘데이터주체통지(data subject notice)’라고 지칭한다.

데이터주체통지를 받은 데이터관리자는 통지를 받은 날로부터 21일 이내에 데이터주체에게 다음과 같은 내용을 포함한 서면으로 된 통지를 보내야 한다.²⁵⁾

- 데이터관리자가 데이터주체통지에 동의하거나 동의할 의향이 있음을 알린다.
- 데이터주체통지의 정당하지 않은 부분과 동의하거나 동의할 의향이 있는 부분에 대한 이유를 알린다.

다음 네 가지 조건 중 어느 하나를 충족시킨다면 개인은 자신의 개인정보에 대해 데이터주체통지를 보낼 수 없다.²⁶⁾

- (동의를 취소한다고 할지라도) 데이터주체가 개인정보 처리에 동의한 경우
- 정보의 처리가 데이터주체청구에서 계약을 맺기 위해 필수적인 경우
혹은 정보의 처리가 데이터주체가 관계자인 계약의 실행을 위해 필수적인 경우
- 정보의 처리가 계약에 의한 의무보다 데이터관리자에게 적용되는 법적 의무에 필수적인 경우
- 정보의 처리가 개인의 이익을 보호하는데 필수적인 경우

이처럼 데이터관리자는 정보공개 중요요청이 타당하다면, 공개를 중지해야 하고 정보처리를 시작해서는 안 된다. 이 때 이 개인정보는 정보공개법 제40조제3항제1호나에 의거해 비공개된다. 만일 데이터관리자가 이 통지가 정당하지 않다고 판단한다면, 21일 이내에 데이터주체에게 통지가 정당하지 않은 이유를 알려야 한다.

데이터관리자는 데이터주체통지를 받은 정보의 공개를 판단할 때 통지의 정당성 여부, 정보공개법의 의무에 따라 정보를 비공개하는 것보다 공개하는 것이 더 큰 가치를 지니는지 여부 등을 고려하여 정보

25) Data Protection Act 1998, Part II s10 (3).

26) ICO, Data Protection Act 1998 Legal Guidance, p.54.

의 공개여부를 신중히 판단하여야 한다.

③ 데이터보호법 제4장 비공개대상정보조항에 해당하는 경우

데이터보호법의 비공개조항에 해당하는 경우에도 정보공개법 제40조제2항에 의거해 정보가 비공개된다. 데이터주체가 데이터보호법의 비공개조항 때문에 주체접근청구를 통해 정보에 접근할 수 없다면 그 정보는 정보공개법의 접근권리에 근거해 다른 어떤 사람도 접근할 수 없다. 정보공개법 제40조는 이 법에 따라 정보에 접근하는 권리는 데이터보호법에 의해 보호받는 권리와 모순되지 않다는 것을 명시하고 있다.

예를 들어 데이터보호법 부칙 7의 첫 번째 항목²⁷⁾은 데이터관리자에 의해 비밀로 제공되거나 제공받는 인물의 신원조회서에 포함된 개인정보 주체접근규정의 비공개조항에 대해 규정하고 있다. 이 신원조회서는 데이터주체의 교육, 훈련, 직원 고용 혹은 미래에 이루어질 교육, 훈련, 고용 등에 대한 정보를 포함하고 있다. 만일 'X'의 전 고용주였던 'A'가 X의 고용 여부를 고민하는 'B'에게 X에 대한 신원조회서를 줬다면, X는 주체접근 청구를 통해 신원조회서의 모든 개인정보에 접근할 수 있는 권리를 가질 수 없다. 데이터보호법 부칙7의 첫 번째 항목에 의해 데이터주체의 접근권이 거부되었기 때문이다. 이 사례에 정보공개법을 적용해보면, 'Y'라는 사람이 공공기관인 A에서 보유하고 있는 신원조회서에 대한 개인정보를 공개 청구한다면, X와 마찬가지로 제40조에 근거해 정보가 비공개될 것이다. 데이터주체 역시 데이터보호법 제7조제1항제3호에 의해 자신의 정보에 접근할 수 없기 때문이다.²⁸⁾

27) 데이터보호법의 비공개대상정보조항 중 제37조에 있는 '그 외의 부수적인 사항들'에 관한 자세한 내용은 부칙 7에 명시되어 있다.

28) <http://www.dca.gov.uk/foi/guidance/exguide/sec40/chap04.htm>.

④ 공인인 제3자의 개인정보공개를 요청한 경우

공인인 제3자의 정보는 제3자의 사적인 생활과 관련된 것인지 공적인 생활과 관련된 것인지 여부를 검토해야 한다. 개인의 가정·가족에 관한 정보, 재정에 관한 정보는 보호받을 수 있다. 그러나 공무 혹은 업무를 수행하면서 발생한 정보는 해당 개인에게 특별한 위험이 되지 않는다면 일반적으로 공개되어야 한다.

일반적으로 직원의 예금계좌내역을 공개하지 않지만 업무거래과정에서 발생한 지출, 급여, 특히 고위 공무원의 상세한 급여내역과 수익 등은 공개하도록 한다. 이러한 정보는 직원의 개인정보에 해당하지만, 국민들이 공공기관에서 세금을 어떻게 사용하는지에 관심을 갖고 있기 때문에 공개해야 한다. 일반적으로 청구정보를 통해 직원들의 이름이 공개될 수 있지만, 하위직 공무원의 이름이 공개되는 것에 대해서는 우리나라에 비해 좀 더 신중하게 판단한다. 하위직 공무원의 이름이나 근무부서가 공개될 경우, 공개정보가 악용되거나 업무에 방해가 될 만한 일들이 발생할 가능성이 고위직 공무원에 비해 더 크기 때문이다. 또한 고위직 공무원일수록 자신의 정보가 공개되는 것을 막을 수 있는 권한이 크기 때문이다.

정보감독관에서 발행한 지침 중 ‘데이터보호전문지침’에서 정보공개법과 관련한 공무원 정보에의 접근에 대해 제시하고 있다. 이 지침에서는 공공기관에서 근무하는 직원의 정보를 공개하기 위해 고려해야 할 여섯 가지 사항을 언급하고 있다.²⁹⁾

- 공개 요청된 정보가 직원의 공적인 생활에 관한 것인가, 사적인 생활에 관한 것인가? 일반적으로 공적인 정보가 사적이거나 민감한 정보보다 공개 기준이 더 낮아진다.

29) ICO, Data Protection Technical Guidance, Freedom of Information: access to information about public authorities’ employees, pp.1~2.

- 공개 요청된 정보는 신원을 확인할 수 있는 개인정보를 삭제하기 위해 수정될 수 있는가? 공개정보의 가치를 훼손하지 않고도 특정 직원의 신원을 확인할 수 있는 정보를 수정하는 것이 가능할 것이다. 그러나 공개 요청된 정보가 명백히 유명한 직원의 업무 활동에 관한 경우, 이 방법은 불가능하다.
- 직원들에게 그들의 정보가 공개된다는 사실을 알렸는가? 그렇다면, 직원들은 자신에 관한 어떤 정보가 공개되는 것을 예상할 수 있는가? 이것은 조직의 특성과 정보 주체인 직원의 근무연수, 조직에서의 역할에 따라 결정된다. 일반적으로 상급 직원과 그들의 업무 기능이 좀 더 빈번하게 공개될 것으로 예상해야 한다.
- 직원이 자신의 정보공개를 거부했는가? 그렇다면, 직원이 공개를 거부한 사유는 무엇인가? 직원의 거부가 반드시 그 정보가 공개될 수 없음을 의미하는 것은 아니다. 그러나 직원에게 자신에 대한 정보공개 요청이 이루어졌으며 거부의사를 고려하고 있다고 알려주는 것이 적절한 방법이다.
- 정보공개로 직원이 어떠한 손해나 불이익을 당할 수 있는가? 손해 가능성은 조직의 특성과 그 조직 내에서 직원의 역할에 따라 결정된다. 예를 들어, 법률 집행부서 직원의 성명을 공개하는 것은 그 직원에게 불이익이 될 수 있다. 공공기관은 공개 결정과 관련해 이러한 위험 정도를 평가해야 한다.
- 공개 요청된 정보가 민감한 내용을 어느 정도 포함하고 있는가? 일반적으로 직원에 대한 민감한 정보일수록, 공개 기준은 더 높아진다. 직원의 건강, 인종이나 민족, 종교적인 신념 혹은 성생활 등의 정보를 어떠한 상황에서 공개해야 하는가를 파악하는 것은 실제로 어려운 일이다.

더불어 이 지침에서는 공공기관에서 근무하는 직원의 정보공개에 관하여 직원들에게도 충분히 고지해야 함을 언급하고 있다. 직원들에게 기관에서 보유하고 있는 정보에 대해 주지시키고, 고위직과 하위직 직원들의 정보에 대한 접근정도가 다르다는 사실을 알려야 하며, 본인의 업무와 관련된 정보가 공개된다는 사실을 알려야 한다. 또한 정보 공개청구를 받았을 경우에 그 정보의 공개로 영향을 받을 수 있는 모든 직원들에게 그 사실을 알리고 공개거부의견을 수렴해서 공개를 고려해야 한다. 이러한 방법들이 모든 기관에 완벽하게 적용될 수는 없지만 적어도 기본적인 사항은 그 조직의 직원 모두 숙지할 필요가 있음을 언급하고 있다.

2) 정보공개법과 데이터보호법에 규정된 개인정보조항 비교·분석

두 법률에서 사용하는 ‘개인정보’ 용어에는 차이가 있다. 정보공개법에서 사용되는 ‘개인정보(personal information)’라는 용어보다 데이터보호법에서 사용하는 용어(personal data)가 좀 더 광의의 의미를 지니고 있다.³⁰⁾

개인정보에 접근하는 방식으로 청구인의 개인정보와 제3자에 대한 개인정보에 대한 접근으로 나눌 수 있다. 정보공개법을 통해 제3자에 대한 개인정보에 접근할 수 있다. 청구인의 개인정보에 대한 접근은 정보공개법 제40조 제1항에 의해 비공개되며 이 경우에 데이터보호법을 적용할 수 있다. 데이터보호법은 데이터주체가 자신의 개인정보에 접근할 수 있는 주체접근권리를 보장해 주체접근청구를 할 수 있도록

30) “Data”는 현실세계로부터 단순한 관찰이나 측정을 통해 수집된 사실(fact)나 값(value)라면, “Information”은 data들의 조합으로 생성되는 것으로 특정한 사용자에게 의미 있고 유용하게 사용할 수 있도록 전환된 정보를 의미한다.

법적으로 보장하고 있다.

‘개인정보의 형태’ 항목에 나와 있는 “공공기관에서 보유하고 있는 모든 형태의 수기기록에 포함된 정보”는 정보공개법에 의해 데이터보호법에 도입되었다. 정보공개법은 공공기관에서 보유하고 있는 정보의 청구에만 적용되기 때문에 그 정보가 어떻게 구조화되어 있는지 여부에 상관없이 공개 청구가 가능하다. 그러나 데이터보호법은 공공기관과 민간기관 모두를 대상으로 데이터주체청구가 가능하기 때문에 민간부문에 청구하는 경우도 고려해야 하는데, 민간조직에서는 데이터보호법에서 정의한 구조화되지 않은 파일링시스템에 보유한 개인정보는 포함하지 않는다.

두 법률에서 규정하고 있는 개인정보공개청구절차는 거의 유사하다. 그러나 정보공개법에 근거한 청구의 경우 청구를 접수한 기관은 접수일로부터 20일 이내에, 데이터보호법에 근거한 청구의 경우 접수일로부터 40일 이내에 청구인에게 답변해주도록 기간을 정했다는 점이 다르다.

정보공개법에 의해 개인정보의 공개를 거부할 수 있는 경우는 동일 청구인이 이미 공개된 정보를 청구하거나 같은 정보에 대해 여러 번 청구하는 경우, 수수료 규정을 초과하는 경우이다. 수수료가 문제될 경우 대다수 공공기관은 청구인에게 청구의 범위를 좀 더 좁혀 중요한 정보에 대한 청구를 다시 할 것을 권고한다. 또한 정보공개법 제40조에 적용되는 경우를 들 수 있다. 데이터보호법에 의해 공개를 거부하는 경우는 동일 데이터주체가 청구한 똑같은 혹은 유사한 주체접근 청구에 대해 이미 청구된 정보를 공개했을 경우, 데이터주체의 개인정보에 제3자에 대한 개인정보가 포함되어 있고 그 제3자가 공개를 동의하지 않았을 경우, 그리고 데이터보호법의 비공개조항에 해당하는 경우를 들 수 있다.

비공개대상정보조항을 살펴보면 데이터보호법은 개인정보를 보호

함과 동시에 데이터주체가 자신의 개인정보에 접근할 수 있는 권리를 보장하지만 국가안보, 범죄와 과세, 의료, 교육, 사회 산업, 연구, 역사, 통계, 출판, 문학, 예술 등 제4장의 비공개조항에 해당할 경우 정보에 접근할 수 없다. 정보공개법의 비공개조항 중 제40조 개인정보조항을 보면 비공개 사유는 데이터보호법과 밀접한 관련이 있다. 제40조 제1항에서 청구인 자신에 대한 개인정보의 공개 청구가 이루어질 수 없다고 규정했고, 제2항에서부터 제3항까지 제3자에 대한 개인정보의 접근에 관한 사항을 명시하고 있다. 제2항 제1호에서는 개인정보의 공개가 8가지 데이터보호원칙에 어긋나면 비공개한다고 규정하고 있다. 제2항 제2호는 제3항의 규정사항을 하나라도 만족시킬 경우에도 비공개된다고 명시했다. 제3항에 나타난 사항을 보면, 데이터보호법 제10조에서 규정한 데이터주체 혹은 다른 사람에게 손실이나 불이익을 초래하는 혹은 초래할 수 있는 정보의 공개, 공공기관에서 보유하고 있는 수기데이터와 관련된 데이터보호법 제33조 제1항에 해당하는 정보의 공개, 데이터보호법 제4장 비공개조항에 해당하는 정보의 공개라는 세 가지 사항 중 어느 하나를 만족시키면 비공개된다.

최대한 명확하게 법률을 적용할 수 있도록 정보공개법은 포괄적이고 추상적으로 개인정보비공개조항을 제시하지 않고 대신 데이터보호법의 조항을 인용했다. 데이터보호법 역시 여러 가지 부칙들을 다양하게 마련함으로써 구체적으로 법률조항을 보완하고 있다. 그리하여 두 법률의 충돌을 최소화하여 적용할 수 있도록 하고 있다. 이처럼 정보공개법과 데이터보호법은 개인정보에 대한 접근에서 상충하기 보다는 서로의 불완전한 부분을 보완하고 조화를 이루면서 청구인과 제3자에 대한 개인정보에의 접근에 영향을 미치고 있다.

5. 맺음말

진정한 의미의 민주주의가 이루어지기 위해서는 국민이 주체가 되어 정치에 관심을 갖고 여론을 형성하여 지속적으로 정부를 감시하고 견제해야 한다. 이를 위해 국민들은 정부 조직으로부터 필요한 정보를 제공 받을 권리를 가진다.

정보공개법의 기본원칙은 공공기관에서 보유하고 있는 모든 정보를 대중에게 공개하는 것이다. 그러나 공개원칙에서 제외되는 상황이 있는데, 이 중에서 개인정보에 관한 사항은 가장 일반적이면서 국민 개개인에게 가장 큰 영향을 미치는 항목이다. 개인의 신원을 확인할 수 있는 정보, 인종 및 민족, 종교적인 신념, 건강 혹은 성생활에 관한 정보 등을 공개할 경우에 개인의 프라이버시 권리를 침해하게 된다.

많은 국가에서 개인의 프라이버시를 보호하기 위하여 개인정보보호법을 제정했다. 개인정보보호법을 통해 국민 개인은 자신의 개인정보를 법적으로 보호 받을 수 있으며 개인정보에 접근할 수 있는 권리, 개인정보가 처리되는 상황에 대해 통보 받을 권리, 부정확하거나 불완전한 개인정보를 수정·삭제·변경하도록 요구할 수 있는 권리 등을 보장 받게 되었다.

많은 국가에서 정보공개법과 개인정보보호법을 제정해 함께 시행하지만 개인정보에 대한 접근에 관해 서로 지향하는 바가 다른 두 법률은 갈등을 일으킨다. 하지만 개인정보의 공개와 보호 기준 사이의 균형을 맞추기 위해 노력하고 있다.

영국 역시 예외가 아닌데, 영국의 경우는 1984년에 데이터보호법이 먼저 제정되었다. 유럽 연합의 95/46/EC 지침 등 국제적인 개인정보보호규범에 따라 데이터보호법이 1998년에 개정되어 오늘날까지 시행되고 있다. 영국의 정보공개법은 다른 나라에 비해 비교적 늦게 제정되

었는데, 유럽연합의 규칙 제1049/2001호 등의 국제적인 정보공개규범의 영향을 받아 2000년에 제정되고 5년간의 준비기간을 거쳐 2005년에 법적인 효력을 발효했다.

이 연구는 영국의 정보공개법과 데이터보호법에 규정된 개인정보 법률조항을 비교·분석하고 개인정보 접근문제에 대한 두 법률의 상호관계에 대해 검토했다. 그리고 개인정보에 대한 공개청구 거부구제 사례에 적용되는 각 법률을 검토하고 사례의 종류와 성격에 대해 분석했다.

개인정보를 공개 청구하는 방식에 따라 데이터주체가 정보 청구인인 개인정보를 청구하는 방식과 정보 청구인이 제3자의 개인정보를 청구하는 방식으로 분류할 수 있다. 그리고 각 경우에 두 법률의 조항이 어떻게 적용되는지 자세하게 검토했다.

첫 번째는 정보 청구인이 데이터주체인 개인정보를 청구하는 경우이다. 데이터보호법 제7조 제2항과 제3항에 규정되어 있는 데이터주체가 자신의 개인정보에 접근할 수 있는 권리인 주체접근권에 의해 개인정보를 청구할 수 있는 주체접근청구가 이루어진다.

두 번째는 정보 청구인이 제3자의 개인정보를 청구하는 경우이다. 정보공개법 제40조에 규정된 개인정보에 대한 비공개조항에 적용되지 않으면 공개가 가능하다. 정보공개법 제40조 제2항과 제3항에 세 가지 비공개사항을 제시하고 있는데, 이 세 가지 사항은 모두 데이터보호법에 규정된 조항을 적용한다. 8가지 데이터보호원칙을 위반하지 않고, 개인정보의 공개가 데이터주체나 다른 사람에게 막대한 불이익을 주지 않고, 데이터보호법의 비공개조항에 해당하지 않는다면 개인정보를 공개할 수 있다.

영국의 법률은 데이터주체의 개인정보공개청구는 데이터보호법에 의해, 제3자에 대한 개인정보공개청구는 정보공개법에 의해 적용될 수 있도록 개인정보의 주체에 따라 확실하게 구분되어 있다. 정보공개

법 제40조에 규정하는 것처럼 데이터보호법을 침해하면 개인정보를 비공개하듯이 두 법률이 같등하기보다 서로의 불충분한 부분을 상대 법률을 활용해 보완하고 있다.

이와 같이 영국의 정보공개법과 데이터보호법은 정보공개 청구주체에 따라 적용되는 법률이 다름을 정확히 명시하고, 참고할 수 있는 자세한 부칙들을 제공함으로써 공공기관에서의 개인정보 처리과정에서 발생할 수 있는 문제를 최소화하기 할 수 있도록 서로 상호 보완적인 역할을 하고 있다.

《참 고 문 헌》

1. 법령

영국 정보공개법 〈Freedom of Information Act 2000〉

[<http://www.opsi.gov.uk/acts/acts2000/20000036.htm>]

영국 데이터보호법 〈Data Protection Act 1998〉

[<http://www.opsi.gov.uk/acts/acts1998/19980029.htm>]

2. 단행본 및 자료집

최정태 외, 《기록관리학 사전》, 과주 : 한울아카데미, 2005

강경근, 《정보공개제도의 입법 및 사법적 실현》, 서울 : 한국법제연구원, 2002

김승태, 《행정정보 공개제도의 집행요인 및 정책효과 분석》, 한국학술정보, 2006

김중량, 《정보공개법》, 서울 : 법문사, 2000

변재옥, 《정보화사회의 프라이버시와 표현의 자유》, 서울 : 커뮤니케이션북스, 1999

유일상, 《언론법제론(개정판)》, 박영사, 2000

최양식, 《영국을 바꾼 정부개혁》, 서울 : 매일경제신문사, 1998

정부혁신지방분권위원회, 《굿 거버넌스 실현을 위한 국민참여적 정보공개제도 활성화 방안 연구》, 행정자치부, 2005

정부혁신지방분권위원회, 《공공역사기록(archives)의 활용과 정보공개》, 행정자치부, 2005

행정자치부 국가기록원, 《주요 외국의 기록관리 관련 법령》, 국가기록원 기록관리혁신단, 2005

Pugh Mary Jo, 설문원 역, 《기록정보서비스》, 서울 : 진리탐구, 2004

Teodore R. Schellenberg, 이원영 역, 《현대기록학개론》, 서울:진리탐구,

2001

Elizabeth Shepherd and Geoffery Yeo, "Managing Records: A Handbook of Principles and Practice", London: Facet Publishing, 2003

Michael Roper and Laura Miller, "The Management of Public Sector Records: Principles and Context", London : International Records Management Trust, 1999

3. 논문

개리 M. 피터슨, 이상민 역, <공개열람 및 개방성>, 《기록학연구》 제4호, 한국기록학회, 2001

경 건, <정보공개를 위한 공공기록관리체계의 정비>, 《법률행정논집》 제8권, 서울시립대학교 법률행정연구소, 2001

_____, <정보공개와 개인정보의 보호: 정보공개법상의 개인정보보호를 중심으로>, 《정보법학》 제6권 제1호, 한국정보법학회, 2002

_____, <정보공개의 새로운 지향: 전자정보공개제도를 중심으로>, 《기록학연구》 제5호, 한국기록학회, 2002

김윤명, <정보공개제도와 지적재산권법>, 《기록보존》 제18호, 행정자치부 국가기록원, 2005

김재홍, <알 권리와 정보공개제도>, 《사회과학》 제10권, 경북대학교 사회과학대학, 2003

김창조, <정보공개법상 비공개사유와 공무원의 비밀엄수의무>, 《공법연구》, 한국공법학회, 2006

설계경, <행정정보공개제도에 관한 연구>, 《외법논집》 제19집, 한국외국어대학교 외국학종합연구센터 법학연구소, 2005

유일상, <국민의 알 권리와 프라이버시의 갈등과 조정 방안>, 《방송과커뮤니케이션》, 문화방송, 2003

- _____, 〈정보공개법상 비공개정보의 범위에 관한 비교법제적 연구 - 한·미·영·일을 중심으로〉, 《헌법학연구》, 한국헌법학회, 2005
- 오향녕, 〈영국 정보공개제도의 발달과 현황: 미완의 여정〉, 《기록보존》 제12호, 행정자치부 국가기록원, 1999
- 이상민, 〈외국의 공공기록정보 공개제도〉, 《기록보존》 제17호, 행정자치부 국가기록원, 2004
- 이원규, 〈행정정보 및 보존기록물 공개의 운영과제〉, 《기록학연구》 제12호, 한국기록학회, 2005
- 이인호, 〈공공부문 개인정보보호법제에 대한 분석과 비판〉 《정보법학》 제6권 제1호, 2002
- 임규철, 〈각국의 개인정보보호법제 비교연구 -미국과 유럽연합의 개인정보보호법제를 중심으로〉, 《공법연구》 제31집 제5호, 한국공법학회, 2003
- 조광희, 〈정보사회에 있어서 개인의 정보공개와 프라이버시 보호와의 관계에 관한 연구〉, 《언론연구》, 중앙대학교 언론연구소, 1997
- 조영삼, 〈정보공개 변화와 몇 가지 논점〉, 제34회 한국기록학회 월례발표회, 2004
- 최정열, 〈인터넷과 개인정보의 보호〉, 《정보법학》 제6권 제1호, 한국정보법학회, 2002
- 하승수, 〈정보공개와 기록관리〉, 《공공기록관리의 새로운 전망》, 한국국가기록연구원 창립5주년기념 심포지엄 자료집, 2003
- 홍성찬 외, 〈프라이버시권과 개인정보보호권〉, 《사회과학연구》 제12권, 건국대학교 사회정책연구소, 1999
- Adam Warren, "Right to privacy? The protection of personal data in UK public organisations", *New Library World*, Vol.103 No.1182/1183,

2002

Lorraine Screene, “How prepared are public bodies for the implementation of the UK Freedom of Information Act, in January 2005?”, *Records Management Journal*, Vol.15 No.1, 2005

Elizabeth Shepherd and Elizabeth Ennion, “How has the implementation of the UK Freedom of Information Act 2000 affected archives and records management services?”, *Records Management Journal*, Vol.17 No.1, 2007

4. 기타 자료

ICO, 2005, Data Protection Technical Guidance, Freedom of Information: access to information about public authorities' employees

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/public_authority_staff_info_v2.0_final.pdf

ICO, 2005, Data Protection Technical Guidance, Subject access requests and legal proceedings

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/subject_access_requests_and_legal_proceedings.pdf

ICO, 2007, Data Protection Technical Guidance, Determining what is personal data

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf

ICO, 2007, Data Protection Technical Guidance Note, Dealing with subject access requests involving other people's information

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/sar_and_third_party_information_100807.pdf

ICO, 2005, Data Protection Technical Guidance, Freedom of Information:

access to information about public authorities' employees

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/public_authority_staff_info_v2.0_final.pdf

ICO, 2007, It's your information, How to access your information

http://www.ico.gov.uk/upload/documents/library/data_protection/introductory/subject_access_rights.pdf

ICO, 2007, Freedom of Information Act Awareness Guidance No.1, Personal Data

http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/awareness_guidance%201_%20personal_information_v2.pdf

ICO, 2007, Freedom of Information Act Awareness Guidance No.3, The Public Interest Test

http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/awareness_guidance_3_public_interest_test.pdf

ICO, 2004, Freedom of Information Act Awareness Guidance No.20, Prejudice & Adverse Affect

http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/awareness_guidance_20_-_prejudice_and_adverse_affect.pdf

ABSTRACT

A Study on the Disclosure and Exemption of the Personal Data*

Kim, Jung Ae

The general public are interested in the politics and form public opinion and keep in check the government for true democracy. The general public have the right to be furnished information from the government. And the government should enact the Freedom of Information Act to provide the public's right to know. At the same time, the government should enact the Data Protection Act to provide the public's right to privacy. There is a friction between the Freedom of Information Act and the Data Protection Act. It's hard to maintain the proper balance between the Freedom of information Act and the Data Protection Act, but many countries try to do so.

The UK enacted the Data Protection Act 1998(DPA), which entered into force on 2000, to comply with EU Directive 1995. The Freedom of Information Act 2000(FOI), which came fully into force on 2005, was passed in 2000. The FOI imposes significant duties and responsibilities on public authorities to give access to the information they hold.

The purpose of this study is to consider the provisions of the personal data in FOI and DPA. Besides this, it identifies the complaint cases on public

* A thesis submitted to the Council of the Graduate School of Kyungpook National University in partial fulfillment of the requirements for degree of Master of Archival Science in January 2008.

authorities about the disclosure and exemption of the personal data in comparison with the acts. If information is the personal data of the person making the request, it will disclose under the DPA. If information is the personal data of a third party, it will disclose under the FOI. These acts interact each other to make up for the weak points in the other to make a proper application of the act on public authorities.

This study may have any limitation in making a comparative study of the disclosure and exemption of the personal data in Korea. But it is expected to provide a basis for understanding the disclosure and exemption of the personal data in the UK.

Key words: Right to know, Right to privacy, Freedom of Information Act of UK, Data Protection Act 1998