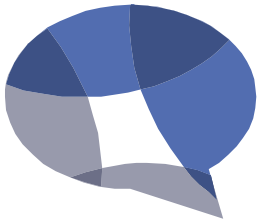
GDPR -지식정보사회에서 국민의 기본권보장 강화

성균관대학교 법학전문대학원
김일환



1. 지식정보사회에서 국민의 기본권보장 강화

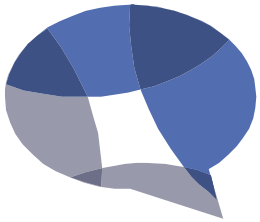
- 오늘날 기본권보호경향은 최대한 기본권을 보호하자는 것 ; 기본권을 절차보장으로 파악하는 것

- 기본권과 조직, 절차를 연결하는 것이 기본권의 실현과 보장을 위하여 아주 중요한 의미를 가짐 더 나아가 지식정보사회에서 개인의 기본권보호는 물론 국가권력행사의 정당성을 위해서도 실체적 기본권은 절차영역에서부터 보호되어야 함

- 전통적인 사후구제제도로는 개인의 권리를 충분히 보호할 수 없음

- 오히려 지식정보사회에서는 국가의 공권력작용으로 인하여 국민의 권리침해가 발생하기 이전에 처음부터 위법하거나 부당한 공권력작용이 행하여지지 아니하도록 예방하는 사전적·절차적 제도를 통한 권리보호 또한 사후적 구제제도만큼 중요해짐

- 사후적 구제제도의 강화와 더불어 사전적 권리보호제도의 신설 및 보강에 대한 검토가 필요함



2. 개인정보보호기술

I. 개인정보보호기술

개인정보보호기술은 개인의 사생활 또는 개인정보를 보호하기 위한 모든 형태의 기술로 정의할 수 있음

일반적인 정보보호기술과 달리 개인정보보호기술은 서비스 자체가 아닌 서비스 이용자를 보호하기 위한 수단으로 설명할 수 있음

개인정보보호기술은 개인정보의 침해를 사전에 예방한다는 측면에서 국민의 기본권인 인간의 존엄, 사생활 비밀의 자유, 개인정보자기결정권의 보호·보장과 관련이 있음

현재 OECD를 비롯하여 미국, EU, 호주, 캐나다 등에서 개인정보 보호를 위한 기술적 설계에 대한 가이드라인을 제시하고 있음

II. Privacy by Design

Privacy by Design은 개인정보를 수집하는 단계에서부터 폐기하는 단계에 이르기까지 이용자의 관점에서 정보보호를 위한 필요한 조치를 취해야 하는 내용(보호조치 관련 조항)과 더불어, 이용자의 권리를 충분히 보장하도록 하는 내용(이용자의 권리 관련 조항) 등을 포함

FTC가 권고하고 있는 Privacy by Design의 기본원칙은 기업으로 하여금 회사조직 전체에서 그리고 자신의 상품과 서비스를 개발하는 모든 단계에서 소비자의 개인정보 보호를 증진시키는 것을 목적으로 하는 원칙임

실질적인 의미에서 이 원칙은 정보보안을 위한 개인정보 보호, 정보수집의 합리적인 제한, 건전한 정보보유 및 폐기관행 그리고 정보의 정확성으로 구성되어 있음

절차적으로는 기업의 상품생산 및 서비스의 생애주기 전반에서 포괄적인 정보관리절차를 수립함

FTC의 관점에서 보면 'Privacy by Design'은 개인정보와 관련된 부담을 소비자에게서 사업자에게로 이전시킨 것으로, 정보주체의 기본권을 보다 강력하게 보호·보장하고 있음

III. 개인정보영향평가

1. 서설

개인정보영향평가는 사전에 개인정보에 대한 영향평가를 실시하여 미리 개인정보 위험요인을 분석하고 이를 초기에 제거하여 개인정보 침해·유출로 인한 피해를 사전에 예방할 수 있도록 고안된 제도임

현행 개인정보보호법 시행으로 도입된 개인정보영향평가는 공공기관에서 개인정보를 활용하는 신규 정보시스템을 도입하거나 기존 개인정보 취급 정보시스템의 중대한 변경사항 발생 시 동일한 시스템의 구축·운영·변경 등으로 인해 개인정보에 미치는 영향을 사전에 조사·예측·검토하는 체계적인 절차를 말함

개인정보를 활용하는 새로운 정보시스템의 도입이나 개인정보 취급이 수반되는 기존 정보시스템의 중대한 변경 시, 해당 시스템의 구축 • 운영 • 변경 등이 개인정보에 미치는 영향에 대하여 사전에 조사 • 예측 • 검토하여 개선방안을 도출하는 절차임

2. 개인정보영향평가 시기

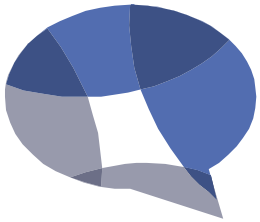
개인정보영향평가는 신규시스템의 새로운 시스템 구축 전단계인 시스템 분석·설계 단계에서 실시하고, 기존시스템의 경우에는 기존 서비스 운영 중 개인정보 수집·이용·관리상에 중대한 침해 위험이 발생할 가능성이 있거나, 개인정보관리 체계 점검·개선이 필요한 경우에 실시함

3. 기업의 개인정보 영향평가 내용

서비스 기획 및 개발 단계부터 개인정보 영향평가를 진행하여 관계법령 준수 여부를 파악하고 영향도를 분석하여 사전에 위험을 제거하고 있음. 개인정보 전문 담당자가 각 단계에서 직접 관여, 서비스 담당자들과 모든 내용을 협의해 개선 방안을 마련함으로써 전사적 개인정보 위험 관리를 함

-서비스 기획에서부터 종료까지 이용자 개인정보가 안전하게 관리될 수 있도록 개인정보에 미치는 영향을 분석함
-서비스 도입 서비스 기획에서 출시까지 개인정보의 라이프사이클 및 개인정보 처리시스템에 대한 적정성을 검토
-서비스 운영 개인정보 수집, 이용 또는 제공의 추가 시 도입 단계의 검토사항을 재검토
-서비스 종료 개인정보 파기 검토 - 파기 시점에 대한 적정성 - 안전한 파기 여부 확인

* 주요 검토 항목
1. 개인정보 수집 - 이용자 동의의 명시성 - 필요 최소한의 수집
2. 개인정보 전송/저장 - 개인정보의 안전한 전송 - 패스워드, 금융정보, 위치정보 등에 대한 암호화 저장
3. 개인정보 이용 - 개인정보의 오 · 남용 예방
4. 개인정보 제공 - 개인정보의 제공의 최소화 - 개인정보의 안전한 전송
5. 개인정보처리시스템 관리 - 개인정보 취급 내역 파악 - 개인정보 취급 권한 검토 - 불필요한 개인정보 노출의 통제 - 개인정보 취급에 대한 로깅



3. 결론

I. ‘개인정보영향평가’와 ‘Privacy by Design’은 모두 개인정보에 대한 정보주체의 기본권에 대한 사전적 권리보호 수단으로써 작용함

II. ‘Privacy by Design’은 기술의 설계를 어떠한 방향과 원칙으로 할 것인지에 대한 내용을 제시하고 있는 반면, 개인정보 영향평가는 정보시스템의 개인정보 침해요인을 파악하고 개선방안을 수립하는 정책적 측면에 대한 제도임

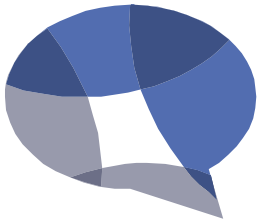
III. 우리나라 현행 개인정보보호법 및 정보통신망법에는 개인정보보호기술에 대한 명확한 규정이 없음

IV. 현재 세계 각국에서 ‘Privacy by Design’이라는 개념을 도입하여 개인정보보호기술의 중요성을 인식하고 있음을 감안해볼 때, 우리 법제 또한 또한 개인정보보호기술에 관한 원칙으로써 ‘Privacy by Design’을 도입하는 방안을 검토해볼 필요성이 있음

VI. 해외 법제들과 달리 개인정보보호기술에 대한 법적 기준을 제시하고 있지는 못하다고 판단됨

VII 우리 법제상 개인정보 보호조치에 대한 규정은 개인정보보호를 위한 기술적 조치들에 대한 규정이지 개인정보보호기술에 대한 원칙 또는 설계 기준까지 제시하고 있지는 못함

VIII. 현행법상 개인정보보호기술 관련된 내용으로는 개인정보영향평가와 안전성 조치의무 규정이 있으나, 개인정보자기결정권의 사전적 보호를 하여 현행 안전성 조치의무 규정 및 개인정보영향평가의 문제점을 보완하고 이와 별도로 개인정보보호기술에 관한 Privacy by Design 원칙을 도입하는 방안을 검토해볼 필요성이 있음



4. 목적구속의 원칙

I. 개인정보자기결정권은 개인에 관한 정보가 존재한다는 사실을 통해서가 아니라 통제되지 못하는 개인정보의 전달 및 원래 수집한 목적과는 다른 목적으로 처리하는 것을 통하여 침해됨

II. 구체적인 목적확정 및 목적구체적인 개인정보의 이용 및 전달을 통하여 이러한 위험에 효과적으로 대처할 수 있음

III. 여기서 우선 구체적인 목적확정 및 원래 수집된 개인정보의 범위 내에 있도록 개인정보처리를 유지시키는 "**목적구속원칙**"이 모든 합법적 정보처리과정을 위하여 중요한 기준으로 작용함

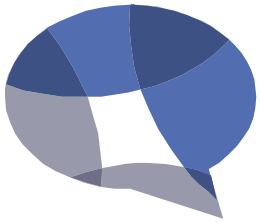
IV. 따라서 개인정보의 이용과 전달 시 요구되는 목적구속원칙은 먼저 개인정보 처리목적의 확정을 요구하고, 계속해서 확정된 목적의 범위 내로 개인정보처리를 한정하는 것을 내용으로 함

V. 목적과는 다른 정보이용 및 처리는 매우 제한된 범위 내에서만 인정되고 법률상 근거를 필요로 하는 새로운 기본권제한이므로 이는 목적구속을 보장하기 위하여 국가기관간 정보전달과 이용에 관한 엄격한 대비책을 필요로 한다는 것을 뜻함

VI. 모든 국가기관은 그들이 갖고 있는 자료나 정보를 갖고서 그들의 과제를 처리하기에 충분하지 않다면 그들의 과제를 이행할 수 있도록 기관 상호간에 원조해야만 하나 이러한 국가기관 상호간 기관협조('행정응원')가 전자정보처리시대에서도 헌법합치적으로 존재할 수 있도록 해야만 함

VII. 그렇다면 특정기관에 저장되어 있는 개인정보가 동시에 모든 다른 행정기관의 공통된 정보를 뜻하는 '정보통일체'가 민주법치국가에서 존재해서는 안 됨

VIII. 결국 국가기관 상호간에 개인정보가 끊임없이 전달되고 이용되는 현실 속에서 이러한 '정보'권력분립원칙과 목적구속원칙을 통하여 관련 개인이 이러한 정보의 전달을 알 수 있도록 그러한 정보이동과정이 공개되어야 함

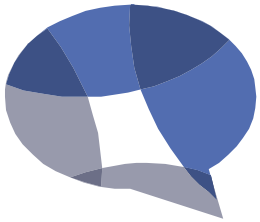


5. 규범명확성원칙

I. 규범명확성 원칙: 자신에 관한 정보가 어떤 구체적인 처리목적들을 위하여 필요한지를 해당 개인이 명확하게 인식할 수 있어야만 한다는 것을 뜻함

II. 따라서 법률의 규범명확성, 조직적이고 절차법적인 예방책들, 관할 기관들의 통지의무, 관련자의 포괄적인 설명청구권 등을 통하여 누가, 언제, 어디에서 어떤 경우에 자기에 관하여 아는지를 관련 개인이 알 수 있도록 보장되어야 함

III. 특히 관련자가 법규정으로부터 그의 개인정보가 어떤 구체적인 행정목적을 위하여 필요한지를 명백히 인식할 수 있어야만 함



6. 투명성

I. 서설

위키리크스(WikiLeaks)가 주로 각국 정부나 기업 등에 조직 속한의 비공개 문서를 공개하고, 에드워드 스노든이 미국 국가안보국(NSA)의 무차별한 도감청을 폭로한 이후 전 세계적으로 개인정보보호에 대한 관심이 높아졌고 글로벌 IT 기업들의 투명성이 강조되고 있음

-구글을 비롯한 글로벌 IT 기업, 네어버와 카카오 등이 2013년 이후 투명성 보고서를 지속적으로 발간하는 이유는 이러한 사회적, 정치적 배경을 바탕으로 하고 있음

II. 투명성의 사전적 의미

- 투명성은 속까지 환히 비치는 성질이나 상황 또는 예측 가능한 상태를 의미함
- 이러한 투명성의 사전적 의미를 법적인 관점으로 전환하여 살펴본다면 명확성, 이해가능성, 인지가능성 내지 예측가능성을 뜻함

어떠한 일의 과정이 투명하다는 것은 그 과정이 널리 개방되어 있다는 것, 즉 감추어진 채 진행되지 않고 이해관계인이나 모든 사람에 의한 간파와 이해가 가능하며 나아가 참여가 보장된 과정을 뜻함

- **결과의 투명성** : 의사결정이나 그에 따른 특정 권한의 행사에 있어 결과가 투명하게 공개될 것
- **절차의 투명성** : 결정이 이루어지는 방식 그 자체의 투명성
- **내용의 투명성** : 모든 정책의 결정과정이 본질적으로 투명하게 이루어질 것을 요구
- **책임의 투명성** : 일정한 의사결정과 그에 따라 발생하는 결과에 대하여 책임의 소재를 분명하게 하고, 나아가 책임을 물을 수 있는 제도적 장치를 마련하는 것을 의미

III. 개인정보보호원칙과 투명성원칙 간 관계

-투명성원칙이 법 상 규정되어 있지는 않으나, 개인정보보호법의 관련 원칙들은 물론 개별 규정들 모두 정보처리의 투명성을 통한 정보주체의 보호를 목적으로 하고 있음

-목적구속원칙 등 개인정보보호를 위한 각종 원칙들과 내용들은 모두 전체적으로 개인정보처리를 정보주체가 가능한 한 이해할 수 있어야만 함을 전제로 하는 바, 결국 이는 투명성원칙에 근거한 것이라고 할 수 있음

-이는 법치주의적 관점에서 요구되는 법질서의 투명성이라는 일반적 차원은 물론 정보주체의 인식가능성을 목표로 하는 개인적 차원도 포함하고 있는 것임

-개인정보자기결정권의 보호를 위해서는 정보주체에게 정보처리가 투명함을 전제로 함

IV. 개인정보와 정보보안 간 관계

개인정보보호에 관한 규정이란 개인정보의 획득 및 처리와 관련되어서 존재하거나 규정되어야만 하는 법규정으로 이해됨

- 정보보안은 개인정보를 보호하기 위한 법률들에 기여하기 위하여 결정되고 이러한 법률들의 준수와 유지를 확보, 보장해야 하며 개인정보의 남용이나 위조방지 등에 기여하는 기술적, 조직적, 절차합치적 보호예방조치라고 이해됨

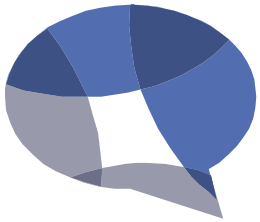
- 따라서 개인정보보호와 관련되어 정보보안은 개인정보보호에 기여하는 기능을 가짐

-우선 어떤 사람이 특정정보에 관하여 통제할 권한을 갖고 있는지에 대하여 우선 법규정으로부터 확인되어야만 함

그 다음에 논리적으로 개인정보에 권한 없는 침입으로부터 보호하는 기술적, 조직적, 절차합치적 정보보안이 언급될 수 있음

개인정보보호는 개인에 관한 정보처리 시 개인정보자기결정권의 제한으로부터 정보주체의 보호를 뜻하는 반면 정보보안은 개인정보를 처분할 개인의 능력보호, 이러한 정보에 권한 없는 인식과 접근으로부터 보호, 정보처리시스템 내에서 이러한 정보의 권한 없는 변경으로부터 보호를 보장해야만 하는 조직적, 기술적 조치로 이해됨

- 개인정보보호란 개인정보를 보호하기 위하여 무엇이 행해져야만 하는 가에 관한 것이고 정보보안은 이러한 정보보호가 어떻게 실현되어야 하는가에 관한 것임



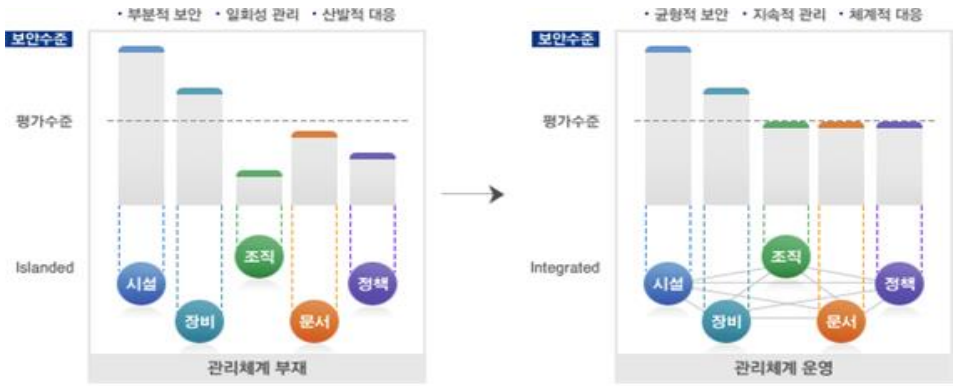
7. 인증

I. 정보보호관리체계 (ISMS)

기업 및 조직이 보유하고 있는 중요한 정보자산에 대한 최적의 정보보호 정책 및 조직수립, 위험관리, 대책구현, 사후관리 등의 업무체계를 종합적으로 평가하는 대표적인 정보보호 인증제도입니다. 2006년 업계 최초로 정보보호관리체계 인증을 취득한 이후, 현재까지 인증을 유지하고 있음

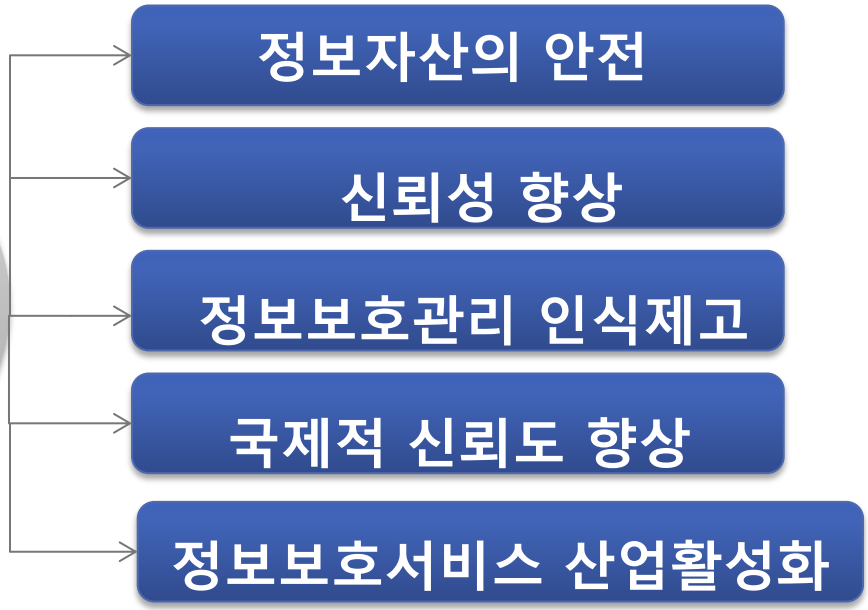
II. 인증제도

1. 서설 : 기업(조직)이 각종 위협으로부터 주요 정보자산을 보호하기 위해 수립・관리・운영하는 종합적인 체계(정보보호 관리체계)의 적합성에 대해 인증을 부여하는 제도



II. 인증제도

2. 목적



3. 법적 근거

"정보통신망 이용촉진 및 정보보호 등에 관한 법률"제47조
"정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령"제50조
정보보호 관리체계 인증 등에 관한 고시
(미래창조과학부 고시 제2013-36호)

III. 개인정보보호관리체계 (PIMS)

이용자의 개인정보를 안전하게 보호하기 위한 다양한 보호대책을 지속적으로 관리, 운영하고 있음을 점검하는 객관성 및 신뢰성이 확보된 대표적인 개인정보 인증제도

※ 기업이 개인정보보호를 위해 무엇을(what to do), 어떻게(how to do) 조치하여야 하는지에 대한 기준 제시

기대효과

-개인정보보호 관리체계 제공을 통한 개인정보 침해 가능성 최소화

-기업이 체계적이고 지속적인 개인정보보호 활동을 수행할 수 있는 방법론을 제공하여, 개인정보 취급자 부주의·관리소홀 등으로 인한 개인정보 침해 가능성 최소화

-국민들에게 개인정보를 안전하게 관리하는 기업을 식별할 수 있는 기준 제공 신뢰할 수 있는 인증 부여를 통해 국민들이 개인정보 제공 여부를 결정할 수 있는 구체적이고도 믿을 수 있는 판단 근거 제거

-국내 기업의 내부정보 및 국부의 해외 유출 방지

-PIMS 인증제도의 도입은 향후 개인정보보호 관련 국내 인증 및 컨설팅 시장의 보호와 해외 인증기관으로의 기업 정보 및 재화 유출 방지

인증체계 구성

IV. 인증체계

-인증제도의 객관성 및 신뢰성 확보를 위해 인정기관, 인증위원회, 인증기관을 분리하여 운영
-인증제도를 관리 · 감독하는 인정기관을 방송통신위원회/행정자치부가 직접 수행 산업계, 학계, 정부의 전문가로 인증위원회를 구성하여 인증결과를 심의
-한국인터넷진흥원을 인증기관으로 지정하여 심사의 객관성 확보

V. 인증운영

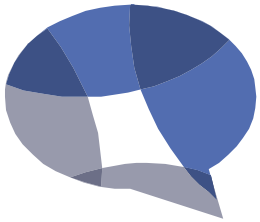
-개인정보보호 관리체계(PIMS) 인증은 기업 자율제도로 운영
-개인정보보호 관리체계를 구축 · 운영하는 기업이 자율적으로 심사를 신청하고, 인증기관이 일정 수준 이상의 기업에 인증을 부여
-개인정보보호 관리체계 인증은 방송통신위원회 고시 제2015-29호/행정자치부 고시 제2015-52호, “개인정보보호 관리체계 인증 등에 관한 고시”를 근거로 운영됨
-인증 취득 시 혜택
-PIMS 인증 취득기업의 개인정보 사고 발생시, 정보통신망법 및 방통위 고시 등에 따라 부과되는 과징금의 경감 고려

* 경감혜택근거 : (과징금) 개인정보보호 법규 위반에 대한 과징금 부과기준(방통위 고시 제2015-30)([별표] 임의적 가중·감경 금액) - "추가적 가중·감경 금액(제8조 관련)"의 감경 사유 및 비율 : 위반 전기통신사업자가 개인정보 보호를 위해 방송통신위원회가 인정하는 인정을 받은 경우 100분의 50이내

VI. 정보보호 인증 일반

- 네이버는 소중한 이용자 프라이버시 및 개인정보 보호를 위해 복수의 공신력 있는 기관으로부터 정보보호 체계를 매년 검증 받고 있음

다양한 네이버 정보보호 관리체계 인증



8. 규제된 자율규제와 행동강령

I. 자율규제의 의의와 구성요소

1. **의의** : 자율규제는 "민간이 자발적으로 또는 국가의 위임에 의하여, 일정한 규율을 필요로 하는 영역 안에서 공익을 수호하기 위한 하나의 질서를 내부적으로 창출하는 것"이라고 할 수 있음 특히 자율규제는 수범자 자신들을 통한 규범의 제정으로서 그 기본이념은 행위기준을 스스로 결정할 수 있는 가능성의 부여에 있음

2. **구성요소** : 자율규제는 자율규범의 정립, 자율규범의 집행, 그리고 자율적 분쟁해결을 포함한다고 할 것

II. 규제된 자율규제의 개념: 규제된 자율규제란 국가가 정해놓은 틀에 따르는 그리고 그 법적인 기초 위에서 작용하는 자율규제라고 할 수 있음. 국가는 자율규제를 가능하게 하는 구조를 마련하고, 경우에 따라서는 규제목표들이 자율규제를 통해 달성될 수 없거나 바람직하지 않은 부작용이 나타날 때 그 정도에 상응하여 자율규제 프로세스에 개입하는 것으로 자신의 역할을 한정함

III. 규제된 자율규제의 핵심요소: 규제된 자율규제에서 국가는 민간의 자율규제를 활성화함으로써 규제기능을 위임하고 더 이상 직접적으로 조정은 하지 않지만 법적 틀을 통하여 상위에 속하는 감시자로서 진행되는 자율규제 과정에 영향력을 행사함.

- 입법의 중점은 구체적인 내용통제에 있는 것이 아니라 집단적인 규범제정을 절차적으로 조종하는 것에 있게 됨

- 따라서 규제된 자율규제에서 국가의 역할은 민간영역의 자율적인 협의를 위하여 법적인 원칙을 세움으로써 절차를 조정하는 것에 중점이 놓이게 됨

IV. 규제된 자율규제의 구현을 위한 국가의 기능:

자율규제에 대한 규제는 법을 통해 직접 이루어지는 것이 아니라, 법에 의해 독립된 감독기구들이 만들어지고 법에 따른 절차를 통해 이 기구들이 해당 영역의 자율규제에 대해 규제와 감독을 수행하는 것

V. 규제된 자율규제의 장점

자율규제는 변화들에 대해서 시간이 많이 소모되는 입법절차를 통해서 국가가 규제하는 것보다 좀 더 융통성 있고 빠르게 반응할 수 있도록 함. 규제된 자율규제의 영역에서는 국가가 감독하는 직접적인 간섭기회가 축소된다. 왜냐하면 해당 영역에서는 자율규제기구에 의한 회원관련 분쟁해결이 우선시되기 때문임. 해당 자율규제기구의 결정이 법률상 부여 받은 권한의 범위 안에 있다면, 관련 국가기구가 개입하거나 또 다른 제제를 부과하는 것이 인정되지 않음

VI. 내용

자율규제기구의 회원이, 당해 자율규제기구가 규정하고 있는 금지된 행동강령들을 위반하게 되면, 당해 자율규제기구는 자체적으로 시정조치 및 징계하거나 또는 벌금이나 제명과 같은 기구 자체의 징벌수단을 행사할 수 있도록 하고 있음

자율규제기구에서 선정한 심사위원의 독립성과 전문성이 보장되어야 하며, 그 결정이 당사자에게 통지되어야 함이 보장되어야 하고, 이의제기수단이 보장되어 있어야 함

VII. 행동강령

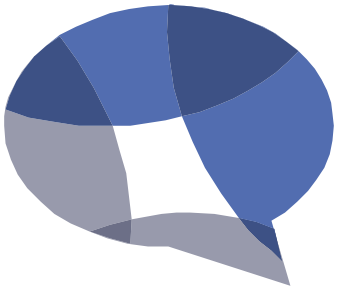
-강령의 목표는 자율규제시스템을 구축하는 것
-이러한 지침들에 포함된 내용들은 입법원칙들에 기반을 두고 있음
-하지만 그들은 새로운 흐름과 기술들에 더 빠르고 더 융통성있게 수용될 수 있다는 이점을 가지고 있음

VIII. 결론

- 헌법과 법률 및 지침 등을 통하여 규제된 자율규제시스템을 도입, 해당 영역의 규제에 관하여 국가와 민간이 공동으로 역할을 분담하여 집행하고 있음을 알 수 있음
- 규제된 자율규제 체제는 국가와 민간의 협력을 제공

- 국가는 법적 기초와 그에 상응하는 구조를 제공

- 바람직하지 못하다고 생각되는 내용들은 국가가 입법과 다른 규제들을 통하여 통제할 수 있음



Thank YOU!