[유럽의 개인정보 보호 관련 법제의 연혁]

ECHR(European Convention on Human Rights)(1951)
Convention 108(Convention for the protection of individuals with regard to the automatic processing of personal data)(1981)
Directive 95/46/EC
Regulation (EC) No. 45/2001(EU Institutions Data Protection Regulation)
Directive 2002/58/EC(Directive on privacy and electronic communications)
Directive 2006/24/EC(Data Retention Directive, 2014. 4. 8. 무효)
Charter (Charter of Fundamental Rights of the European Union)
Regulation (EU) 2016/679 (General Data Protection Regulation)
Directive (EU) 2016/680 (Criminal Enforcement Directive)

[GDPR의 구조]

I. 일반 규정
II. 원칙
III. 개인정보주체의 권리
IV. Controller, Processor
V. 개인정보의 제3국 또는 국제 조직으로의 이전
VI. 독립감독기구
VII. 협력과 일관성 유지
VIII. 구제, 책임, 벌칙
IX. 특별한 상황의 처리에 관한 규정
X. 하위 법률과 이행 법률
XI. 최종규정

[적용 범위]

1. 목적

2. 대상

가. 적용대상

- automated mean
- filing system

나. 적용제외

- 연합 법률 적용 대상이 아닌 것
- 공동방위, 외교

- 순전히 개인, 가사 범위
- 범죄 수사, 형사 집행 등
  - 특별규정(Directive 2016/680)
  - 그 밖에는 GDPR

3. 지역

가. Establishment in the Union

나. Not established in the Union, activities are related to
- Offering of goods or services
- Monitoring of their behavior

다. public international law

[개인정보란 무엇인가?]

1. GDPR의 규정[1]

> 4(1) 'personal data' means any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;
> 참고 Directive 95/46은 : 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

2. 폭 넓은 정의와 유연한 적용, 회색지대를 포함할 수 있어야 함

- 모든 정보를 포함하도록 하는 것이 목적이었음. – convention 108의 정의
- 정의는 넓게, 적용은 유연하게
- 넓어서 기술 진보를 예측할 수 있어야 하고, 그 범위 안에 회색지대를 모두 포함할 수 있어야 한다.(5페이지)

3. 요소

가. 모든 정보(“any information”)

[1] 개인정보보호법 : "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

가. 모든 정보 : 넓게 하려는 의도(clearly signals the willingness of the legislator to design a broad concept of personal data)

나. 성질(Nature) : any sort of statements about a person.

- "objective" information, such as the presence of a certain substance in one's blood.
- "subjective" information, opinions or assessments.
  - ◆ banking, for the assessment of the reliability of borrowers in insurance in employment
- it is not necessary that it be true or proven.
- incorrect

다. 내용(Content)

- any sort of information.
- 평가나 의견
- 사생활, 개인적인 것, 가정 내의 것 – 민감한 정보
- 그에 국한하지 않고, 직업, 경제적, 사회적 행동에 관한 것도 포함(C-101/2001, Lindqvist).
- 직업적 습관이나 행위 – 의사나 약사의 처방(환자 이름이 익명이라도)
- labour law (Article 8.2 (b)), criminal convictions, administrative sanctions or judgements in civil cases (Article 8.5) or direct marketing (Article 14 (b)).

라. 형식이나 매체(Format or medium)

- 알파벳, 숫자, 그래픽, 사진, 음성. 종이, 컴퓨터 메모리, 비디오 테이프. 음성, 이미지(33조[2]),
- 텔레뱅킹, 비디오 감시, 어린이의 그림

마. 생체정보

- 개인에게 고유하고(unique), 측정 가능한 생체적 특징, physiological characteristic, 반복 행동, living trait.
- 지문, 홍채, 안면 구조, 음성, 손금, 정맥 패턴, 능숙한 기술, 행동 특징(서명, 특정한 걷는 행태, 말하는 습관, keystroke)
- content이며, 식별자.

[2] The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.
(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

나. ~에 관한(“relating to”)

(1) About
- 자명하기도 : 특정인의 진료카드, 인사기록 등.
- 개인들이나 객체들
- 부동산의 가격
- 자동차 정비서비스 기록
- RFID

(2) 3가지 요소 평가

3 요소(3 elements) 테스트(WP 136)
- 내용(content) – 목적이나 미치는 영향과 무관하게 특정 정보가 어떤 사람에 대한 것일 때.
  - ■ 예를 들어 특정인의 의료기록의 검사결과나 분석결과, 인사카드의 기록 등.
- 목적(purpose) – 개인을 평가하거나, 개인에 대한 처우, 개인의 상태나 행동에 영향을 주는 목적으로 사용될 경우.
  - ■ 예를 들어 어떤 회사의 전화 통화기록은 목적에 따라서 회사에 관한 정보(요금청구의 관점), 직원에 대한 정보, 청소 관리자에 대한 정보가 될 수 있다.
- 결과(result) – 내용이나, 목적 요소가 없어도 특정인의 권리나 이익에 영향을 주는데 정보가 사용될 수 있는 경우 특정인에 관한 정보로 볼 수도 있다.
  - ■ 예를 들어 택시 회사가 기사가 아닌 택시 위치를 파악하여 고객 요청에 따라 배차할 경우, 목적이나 내용이 택시 기사와 관련 없어도 택시 기사에 영향을 주므로 택시 기사에 관한 정보
- 3가지 요소를 모두 고려해야 함. 각 요소에 따라 여러 사람의 개인정보가 될 수도 있음. 개별적으로 판단해야 함. 예를 들어 다수가 참여한 회의의 회의록.

다. “an identified or indentifiable”

(1) 식별되는 : 한 사람을 가려낼 수 있는

(2) 직접 또는 간접적으로(directly or indirectly) 식별될 수 있는(identifiable)
- 직접 : 이름
- 간접 : 전화번호, 차량 번호, SSN, 여권번호, 몇 가지 정보들
- Single out : 구체적인 상황에 따라서. 예를 들어 ‘검은 옷을 입은 사람’도 상황에 따라서 개인이 식별될 수 있음.

휴대전화번호 뒷자리 4자리는 개인정보임
사실관계 : 경찰공무원인 X가 A의 신고에 따라 B 등의 도박 현장을 단속한 다음 훈방 조치하였는데, 그 후 B로부터 신고자의 전화번호를 알려 달라는 부탁을 받고 A의 휴대전화번호 뒷자리 4자'를 알려 줌. A가 청문감사실에 X가 신고자를 B에게 알려줬으니 조사해 달라고 신고하자, 허위사실을 유포하고 있다고 진정함.
판결 : 휴대전화번호 뒷자리 4자만으로도 그 전화번호 사용자가 누구인지를 식별할 수 있는 경우가 있고, 특히 그 전화번호 사용자와 일정한 인적 관계를 맺어온 사람이라면 더더욱 그러할 가능성이 높다. 본 건에서도 B는 4자리를 자신의 휴대폰 통화내역으로 검색하여 신고자를 알아냈다. 따라서 개인정보임. (대전지방법원 논산지원 2013. 8. 9. 선고 2013고단17 판결)

(3) controller 또는 제3자가 활용할 수 있을 것으로 합리적으로 예상되는 모든 식별 수단

- all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.
- 객관적 요소(비용, 시간), 기술(처리 당시, 기술 발전 고려)
- 이해관계
- 보존기간과 기술발전 고려(1개월 보관인 경우와 10년 보관인 경우의 차이)
- 목적도 고려 : 식별의 목적(CCTV)

라. "natural person"

- 생존하는 개인을 의미함.
- 사자의 정보가 생존하는 개인에 관한 정보일 경우
- 사자에 대한 개인정보보호 필요성. 회원국은 사자에 대한 개인정보 처리 규칙을 정할 수 있음(GDPR Recital (27)) .
- 태아의 경우
- 법인의 경우 : 개인에 대한 정보가 될 수도 있음. 회원국 중 법인에 대해서까지 보호를 넓힌 나라도 있음.

마. Recital (30)

Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

- 온라인 identifier : 기기, 애플리케이션, 툴과 프로토콜(예를 들어 ip 주소), 쿠키 identifier, rfid tag 등.
- IP 주소 : 개인정보에 해당(WP 37). 특정하게 취급하기 위해서 수집, 관리.

<가명화, 익명화, 비식별화 논란에 대하여>

1. 익명화 기술, 가명화 기술과 재식별 가능성

가. 익명화 기술

- 익명화 기술은 크게 무작위화(randomization) 방법과 일반화(generalization) 방법[3]
- 무작위화 방법에는 잡음 추가 방법, 순열 방법, 차등 정보보호 방법(Differential privacy), 대체 등이 있다고 함.
- 일반화 방법에는 총계처리(Aggregation)와 K-익명성(K-anonymity) 방법, l-다양성 (l-diversity)/ T-근접성(T-closeness) 등의 방법이 있다고 함.

나. 익명화 기술의 재식별화의 위험

- 익명화 기술 자체가 식별가능성을 줄이는 것이기 때문에, 대부분의 익명화를 위한 기술들은 재식별화의 가능성이 있음.
- 익명화 기술에서 재식별화의 가능성은 3가지 측면. Single out(개별화), Linkability(연결 가능성), Inference(추론 가능성)
- 아무리 익명화를 위한 처리를 하더라도, 거의 모든 경우 재식별이 가능하다는 것이 최근의 연구 결과.
- 실제로 최근 유럽에서 휴대폰 정보를 활용하여 재식별이 가능한지를 분석한 사례가 있는데, 연구자들이 작은 유럽 도시에서 150만 휴대폰 이용자들의 정보를 15개월 동안 연구하였는데, 단지 4개의 힌트만 있다면 그들의 95%를 식별해 낼 수 있었다는 결과를 발표. 100만명이 넘는 사람들의 익명화된 정보에서 1년에 4번의 아주 정확하지 않은 위치 정보만 가지고 있어도 개인을 식별해 낼 수 있었다고 함.
- 각 익명화, 가명화 기술의 개별화, 연결가능성, 추론가능성에 의한 재식별가능성의 정도를 도식화한 것.

	Is Singling out still a risk?	Is Linkability still a risk?	Is Inference still a risk?
Pseudonymisation	Yes	Yes	Yes
Noise addition	Yes	May not	May not
Substitution	Yes	Yes	May not
Aggregation or K-anonymity	No	Yes	Yes
L-diversity	No	Yes	May not
Differential privacy	May not	May not	May not
Hashing/Tokenization	Yes	Yes	May not

(출처 : 유럽연합 29조 작업반, Opinion 05/2014 on Anonymisation Techniques, 24 페이지, 2014년 4월 10일)

- 익명화 기술로 익명화 처리를 하더라도 기술 발전에 따라 재식별화를 위한 비용

[3] 유럽연합 29조 작업반, Opinion 05/2014 on Anonymisation Techniques(2014년 4월 10일), 12 페이지

이 계속 낮아지고, 재식별화를 위해 가용한 정보가 증가하여 재식별화 가능성이 지속적으로 높아진다는 점도 고려해야 함. 기술은 현재의 기술 뿐만 아니라, 기술의 발전가능성도 고려해야 함.[4]

2. 가명화에 대한 GDPR 규정

가. 규정

4(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
Recital (26) Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.
(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.
(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.
25 **Data protection by design and by default**
1.Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

나. 가명처리된 정보의 취급

- 여전히 개인정보로 취급
- 가명처리 정보라는 개념을 도입한 것이 해당 정보에 대한 개인정보 보호를 배제하려는 것이 아님(recital 28 : The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.).

다. 가명처리는 개인정보 보호를 위한 수단으로만 언급

- 설계 단계부터 프라이버시 고려
- 보안
- 아카이빙 목적

[4] 위 자료 8 페이지

- Code of conduct

3. 익명화에 대한 GDPR 규정

가. GDPR 규정

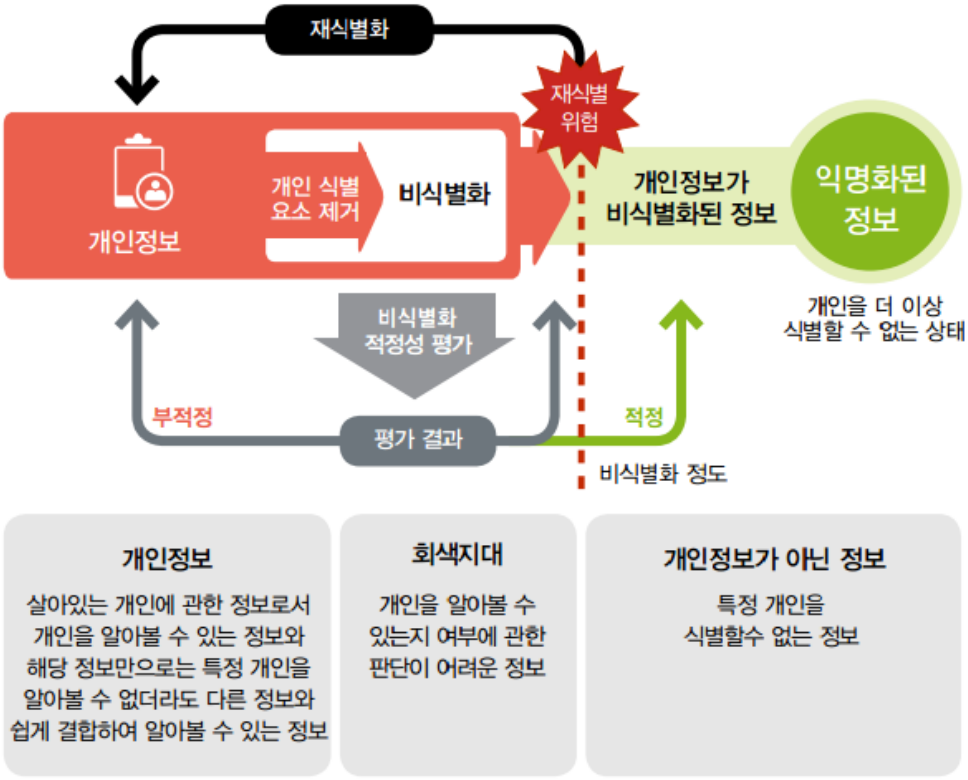
> Recital (26) The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

- 익명화에 대해서 별도의 정의 규정을 두지 않고, recital에서만 언급함.
- 더 이상 식별할 수 없는 것(no longer)
- 유럽연합 Working Party 29도 재식별화(re-identification)의 가능성 때문에 오해를 줄 수 있는 익명성(anonymity)이나 익명 정보(anonymous data)라는 표현보다는 익명화 기술(anonymisation technique)이라고 표현함.
- Directive 95/46 EC도 정식 규정에는 포함시키지 않고, Recital 26.에 익명화된 데이터(data rendered anonymous)에 대한 표현을 두고 있다. 여기에서도 '비식별화 정보는 개인정보가 아니다'라는 규정을 두지 않고, 개인이 더 이상('no longer possible') 식별될 가능성이 없다면. 개인정보로 보지 않는다고 표현하고 있다.

4. 비식별화

가. 비식별화라는 용어는 오해의 소지가 있는 잘못된 용어임

- 비식별화는 식별의 모순 개념으로 회색지대를 고려하지 않는 잘못된 개념이다.
- 비식별화가 아닌 식별불능화나 익명화가 적당한 용어임.



(출처 : 개인정보 비식별화에 대한 적정성 자율평가 안내서, 25 페이지)

나. 익명화라는 용어가 더 적절함

[주체들 : Controller, processor, recipient, third party[5]]

1. 개인정보의 처리와 관련된 주체들

가. controller : 목적, 처리 방법 결정

(1) 개인정보파일의 controller → 결정권을 갖는 자
(2) 단독 또는 공동으로
(3) 최초로 개인정보 수집을 결정하고, 그와 같이 하는 법적 근거를 갖는 자

[5] (d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;
(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(4) 개인정보 항목, 내용, 목적, 대상. 누구에게 공개할 것인지, 왜 공개하는지, 보유기간, 수정 주기 등

나. processor

(1) Controller를 위하여 처리를 하는 자
(2) 어떤 IT 시스템을 사용할 것인가, 어떻게 저장할 것인가? 어떤 보안 시스템을 사용할 것인가, 전송 수단, 검색 방법, 삭제 방법 등을 결정.

다. 수령자

(1) 개인정보를 받는 상대방. 제3자 여부 불문.
(2) 수령자가 제3국에 있을 경우

라. 제3자

(1) 정보주체, controller, processor, 그들의 직접적인 지휘를 받는 자가 아닌 자로서 개인정보를 처리하도록 허용된 자

2. 우리나라의 경우

가. 개인정보처리자

나. 개인정보취급자

다. 정보통신서비스제공자, 이용자
- 정보통신망법 제22조 제1항 전문에 의하여 보호되는 개인정보의 주체인 이용자는 자신의 개인정보를 수집하려고 하는 정보통신서비스 제공자로부터 정보통신서비스를 제공받아 이를 이용하는 관계를 전제로 하고 있다고 해석된다.

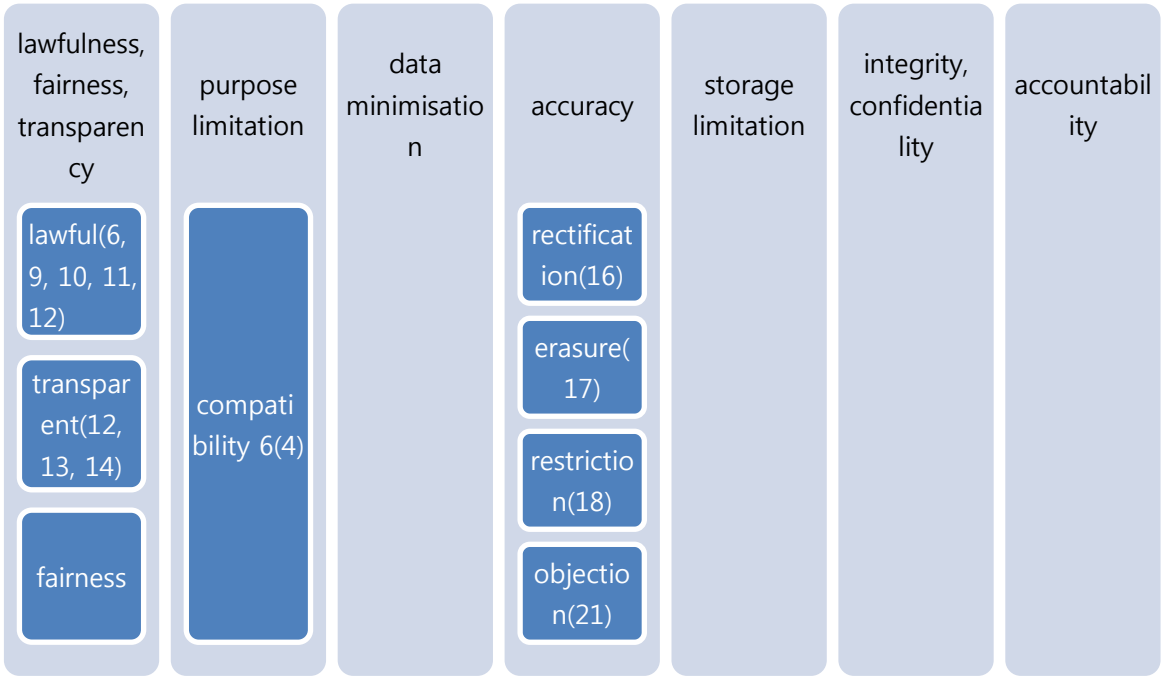
라. 위탁자, 수탁자

[개인정보 처리의 원칙]

1. 규정

Principles relating to processing of personal data
1. Personal data shall be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject **('lawfulness, fairness and transparency')**;
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (**'purpose limitation'**);
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**');
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('**storage limitation**');
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**').
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability**').

2. 각 조문과의 관계



3. GDPR 개인정보 처리 원칙의 특징

가. 적법성을 평가하는데 실질적인 역할을 함

- Directive 에서도 마찬가지임
- 우리나라 개인정보보호법 제3조에 개인정보 보호원칙이 있지만, 개별 규정으로 구체화되어 있지 않은 원칙은 어떤 효력이 있는지 문제[6]
  - ■ 예를 들어 제6항의 사생활 침해 최소화 처리, 제7항의 익명처리 원칙

나. 중복 적용

[투명성]

> The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.

[목적 제한]

> collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

1. 연혁

[6] 제3조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
⑦ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.
⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

가. European Convention on Human Rights : 프라이버시의 합리적 기대

나. Convention 108 : 목적 제한의 원칙 규정, incompatible 개념도 도입.

다. OECD Guidelines : purpose specification and incompatibility

라. Directive 95/46/EC : explicit 요건 추가

2. purpose specification('specified, explicit and legitimate' purposes)

가. quality of data 의 사전 요건

- 수집, 처리되는 개인정보의 충분성, 적절성, 비례성, 정확성, 보유기간 판단의 기준

나. specified

- 핵심적 지위
- 시점 : 수집시
- 명확성, 얼마나 자세하게 : 사용환경 개선, 마케팅 목적, 보안 목적, 사후 연구 목적 등은 모호함. 수집과 개인정보의 맥락에 따라 판단
- 하나 이상의 목적인 경우 : 분명하게 구별되게

다. 명시적(explicit)

- 명확하게 드러나고, 설명되거나 표현되어야 함.
- 모호하지 않게.
- 정보주체에게

라. 목적은 합법적이어야

3. compatibility

가. 추가적인 처리

- 최초 수집시의 목적과 다른 구체적인 목적
- 후속 처리 목적

나. 양립할 수 없는

- 다른 목적이라도 양립 가능할 수 있음.

다. 사례

- 추가적인 처리가 명백하게 예측될 수 있는 경우
- 양립할 수 없는 경우
- 다소 불명확한 경우

라. 양립가능성에 대한 평가 요소

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
(d) the possible consequences of the intended further processing for data subjects;
(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

(1) 최초 수집 목적과 추가 처리 목적의 관계
(2) 수집 당시의 맥락과 정보 주체가 추가적인 활용에 대한 합리적 예측
(3) 개인정보의 성격
(4) 추가 처리가 정보주체에게 미치는 영향
(5) 정보처리자가 공정한 처리와 부적절한 영향을 방지하기 위한 보호조치

마. 역사, 통계, 과학 목적의 추가적인 처리

(1) 다양한 맥락과 그에 따른 개인정보 주체의 영향
(2) 그에 따른 다양한 보호조치

바. 양립불가능한 추가 이용의 상황

(1) 양립불가능한 추가 이용
(2) 이 경우 새로운 적법한 처리 요건을 취하는 것은 규정의 잠탈

[최소 수집과 보관 제한]

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

[적법성 - 적법한 처리]

1. 연혁

가. ECHR(1950) – privacy

나. Convention – privacy, data protection

다. OECD 가이드라인 – lawful, 동의

라. Charter – privacy, data protection, 기준

마. Directive – 6가지

바. GDPR – 6가지

2. 개요

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point
(f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

- 6가지[7]
- 동의
- 계약
- 법적 의무
- Vital interest
- Public task
- Legitimate interest

[적법성 요건 : 동의]

1. GDPR에서 동의

가. 합법적 처리의 요건(6.1(a)) – '동의'
나. 아동의 경우(8.1) – 법정 대리인의 동의가 추가적으로
다. 특정한 유형의 개인정보 처리의 요건(9.2(a)) – 명시적 동의(explicit consent)

2. 동의와 개인정보 처리의 원칙

(1) 동의를 받았어도 개인정보 처리에 대한 원칙(5조)은 적용됨.
동의를 얻었어도 과도한 수집은 위법함(15/2011 WP Opinion) .
(2) 완전히 유효한 동의라도 정보controller의 의무를 경감시키거나, 개인정보 처리에 대한 원칙(5조)에 의하여 불공정(unfair)한 처리를 적법한 처리로 만들지는 않는다.

3. 동의란?

4 (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

가. any indication

(1) 형식은 제한 없음. 서면. 주체의 의지(wish)를 명확하게 나타내려는 표시라면 행동도. Ex) 통에 명함을 넣는 행동.

[7] 제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

(사례) 블루투스 광고 서비스와 개인정보 이용에 대한 동의

(2) 행동을 하지 않는 것을 동의로 볼 수 있는가?
(3) 수동적 수용을 동의로 볼 수 있는가?

나. affirmative action, unambiguous

(1) GDPR에서 추가됨.
(2) 적극적인 행동. 서면 진술, 구술, 전자문서로 진술.
(3) 박스 체크, 기술적 설정의 선택, 기타 정보주체의 정보처리에 대한 수락의 의사를 명백하게 보여주는 행동이나 표시.
(4) 침묵, 미리 박스에 체크된 것, 가만히 있는 것은 동의로 볼 수 없다.
(5) 전자적으로 동의를 요청하는 경우에는 동의 요청이 명확하고, 간결하고, 제공하는 서비스 이용에 불필요하게 혼란을 일으키는 것이어서는 안된다.
(6) 묵시적 동의(implied consent) : '서비스를 사용하는 경우 동의한 것으로 본다'는 묵시적 동의를 명백히 배제하는 것.

다. freely given

(1) 자유롭게 동의 여부를 선택할 수 있어야 한다(genuine and free choice)
(2) 손해 없이 동의 거부나 철회가 가능해야 한다.
(3) 7(4) : 서비스 제공이 당해 계약의 이행에 필요하지 않은 개인정보 처리에 동의하는 것을 조건으로 하는 경우는 자유로운 선택권이 주어지지 않은 것임.

Recital 43 : 개인정보를 나누어서 동의할 수 있게 하거나, 필수적이지 않은 개인정보 처리에 동의하지 않으면 서비스 제공이 되지 않는 경우는 자유 선택권이 없는 것임.
Recital 43 : 정보주체와 정보controller 사이에 뚜렷한 불균형이 있을 때 정보주체로부터 동의를 받는 것을 해당 개인정보를 처리할 수 있는 합법적 근거로 삼아서는 안된다. 특히 공공기관의 경우에 정보주체의 동의는 자유스럽게 이루어진 것으로 보기 어렵다.

(4) 의료 서비스에서 사회적, 재정적, 심리적이거나 그 밖의 어떤 유형의 유인이 없는 상태. 동의를 하지 않으면 치료 거부나 낮은 수준의 치료와 같이 위협이 있는 상태에서 동의를 받는 것은 자유로운 동의가 아니다. (WP 131, opinions on electronic health records)[8]

[8] "free consent means a voluntary decision, by an individual in possession of all of his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological or other. Any consent given under the threat of non-treatment or lower quality treatment in a medical situation cannot be considered as 'free' ... Where as a necessary and unavoidable consequence of the medical situation a health professional has to process personal data in an EHR system, it is misleading if he seeks to legitimise this processing through consent. Reliance on consent should be confined to cases where the individual data subject has a genuine free choice and

(5) 고용의 경우 노동자는 동의를 거부할 가능성이 없는 것은 아니지만, 실질적으로는 동의를 거부하는 경우 취업 기회를 잃을 수 있다. 이런 상황에서 동의는 자유로운 동의가 아니며, 유효하지 않다. (WP48 on the processing of personal data in the employment context)[9]
(6) Ad Blocker 사용을 금지하는 경우는 문제가 있을 수 있음.
(7) 철회도 동의처럼 쉬어야 한다(7(3)).

라. 특정된, 고지된(Specific and Informed)

(1) 특정되어야 함. 다른 동의나 행동과 나눠서 별도로 받아야 함.
(2) 투명해야 함.
(3) 고지되어서 알아야 함. 최소한 처리의 목적, 정보controller가 누구인지, 정보주체의 권리가 무엇인지 등이 고지되고, 알아야 함.[10]
(4) 그렇지 않으면 동의를 받은 것으로 볼 수 없음.

4. 동의의 조건

> Article 7 Conditions for consent
> 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
> 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
> 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
> 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

가. 입증할 수 있어야

- 입증책임은 동의를 받는 측.

나. 다른 것과 함께 서면 동의를 받는 경우

---

is subsequently able to withdraw the consent without detriment."

[9] “"where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 as it is not freely given. If it is not possible for the worker to refuse it is not consent…. An area of difficulty is where the giving of consent is a condition of employment. The worker is in theory able to refuse consent but the consequence may be the loss of a job opportunity. In such circumstances consent is not freely given and is therefore not valid. The situation is even clearer cut where, as is often the case, all employers impose the same or a similar condition of employment.”

[10] Article 13 Information to be provided where personal data are collected from the data subject

- 분명하게 다른 것과 구별되게
- 알기 쉽고, 쉽게 접근할 수 있는 형식, 명확하고 평이한 말로
- 정보주체가 동의하는 내용에 대해서 알 수 있도록 해야 함. 사전에 정보처리자가 동의할 문안을 작성해 놓은 경우는 Council Directive 93/13/EEC에 부합해야(should be provided in an intelligible and easily accessible form, using clear and plain language). 불공정한 조항이 들어 있으면 안됨.

다. 규정을 위반하는 내용에 대한 동의

- 무효

라. 철회할 권리

- 언제든지 철회할 권리
- 기존의 처리에는 영향을 미치지 않음
- 동의를 받을 때 철회할 수 있다는 점을 알려야
- 철회는 동의와 같이 쉬워야

마. 자유로운 동의인지의 판단 기준

- 계약 이행이나 서비스 제공이 계약 이행에 필요하지 않은 개인정보의 처리를 조건으로 하는 경우는 자유로운 계약이 아님.

바. 공공부문과 동의

사. 시점

- 사전 동의

5. 동의의 역할

- 적법한 이해 : 계약의 체결에 따른 필수 정보
- 동의 : 그 외의 추가 정보

각 경우 동의는 적법한가? 자유로운가?
- 의료 분야 : Electronic Health Record
- e-Government
- 수사, 경찰
- Body Scanner
- PNR(Passenger Name Record) Data

[아동의 동의]

1. GDPR

Article 8 Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.
2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.
3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

2. GDPR에 처음 규정을 둠

- 그 동안 지속적으로 아동의 보호를 위한 동의 규정의 필요성이 제기됨
- 각국의 기준이 달라서 혼란이 있었음.
- 그 동안의 WP 29의 의견서 등에서 제안된 내용을 규정으로 둠.

3. 아동과 개인정보보호

- 정보사회서비스(수신자의 요청으로 원격으로 전자적 수단으로 이루어지는 서비스)를 직접 아동에게 제공하는 경우로서 6(1)이 적용될 때 아동이 16세 이상이어야 적법한 처리를 할 수 있다. 16세 미만일 경우 친권자의 동의가 있는 범위에서만 적법. 13세까지 낮출 수 있다.
- controller는 친권자의 동의나 승인을 확인하기 위한 합리적 노력을 하여야 한다. 기술적 수준을 고려하여.
- 1항은 아동과 관련한 계약의 유효성, 형식, 효력에 대한 회원국의 일반적인 계약법에 영향을 미치지 않는다.

[적법성 요건 – 계약, 법적 의무, 필수적 이해, 공무 수행]

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

1. 계약

가. 계약 이행에 필요한 경우

(1) 해석
- 엄격하게 해석해야 함. 진실로 계약 이행에 필요한 경우이어야 함.
- 프로파일링을 하는 것은 필요한 경우로 보기 어려움.
- 그 내용이 계약서에 작게 인쇄되어 있었떠라도 필요한 것으로 보기 어려움.

(2) 목적 제한의 원칙, 필요성 원칙과 관련성
- 계약의 중요하고 본질적인 목적이 무엇인지를 해석하는 것이 중요.
- 피용자에 대한 연락처 정보망 구축시
- 고객에 대한 감시
- 피용자에 대한 비디오 감시

(3) 계약 이행이 아닌 불이행에 대한 후속조치에 필요한 경우
- 해당 조항이 적용될 수 없다고 봄.
- 고객의 기본정보는 계약 이행에 필요하다고 보지만, 채권 추심에 필요한 정보는 legitimate interest의 요건을 충족하는 경우(충분한 보호조치 수반시)

나. 계약 체결 이전 – 정보주체가 요청하는 경우 사전 절차
- 청약 요청시, 제한적 기간 동안
- 견적 요청시
- 상세한 신용도 체크나, 건강 체크는 legitimate interest 요건 평가
- 먼저 DM을 보내는 것, 프로파일링, 행태 광고, 제3자와 공유는 요건 해당 안됨.

2. 법적 의무

가. 처리자가 법적 의무 준수 위해 필요한 경우
- 사회보장, 조세, 경쟁 당국, 개인정보 감독 등
- 공공기관의 업무 수행을 위해 필요한 경우보다 엄격

나. 법률에 의한 의무이어야 함

- 해당 법률은 다른 요건 충족해야 함, 필요성, 비례, 목적 제한 등

가. 개인정보 주체나 제3자의 vital interest

- 생명, 상해, 건강 침해
- 민감정보인 경우는 해당자가 신체적 또는 법률적으로 동의를 할 수 없는 경우. 그러나 이 경우도 동의를 받을 수 있다면 동의를 받도록 해석하는 것이 바람직.
- 예를 들어 대규모 전염병, 보안 사고

나. 필요한 경우

4. Public task

가. 공익(public interest)을 위한 업무 수행
- 처리자가 공공기관 또는 공익적 활동
- 세무 당국
- 변호사 단체(공익 업무)
- 정부 기관이 요구하는 경우도
- 자발적으로 하는 경우도

나. 공적 권한(official authority) 행사
- 아웃소싱 증가로 해당 사유 많아짐.

다. 법률

라. 필요한 경우

마. 목적은 그 범위

바. 비례 원칙

[적법성 요건 – 합법적 이익 Legitimate interest]

1. 규정

2. 성격

가. 다른 요건들과의 관계

- 마지막
- Open door
- Last resort vs 덜 엄격한 요건? 별개의 요건?
- 적절하게 활용되어야 함
- 5가지 요건은 충족하면 적법한 것으로. 그러나 마지막 요건은 특정한 테스트를 통과해야
- 테스트 요건은 오히려 정보주체를 보호하는 것으로 활용될 수도 있음. 따라서 가장 약한 고리가 아님.
- 6호의 가치는 균형 접근. 처리자와 정보주체 모두에게.
- 중복될 수 있음
- 6개의 요건은 동등. 6번째가 보충적인 것은 아님. 6번째 요건에 대해서 특별히 엄

격한 투명성, 책임성을 부여하여야 한다는 견해도 있음(의회 제안).

나. 유연성

- open ended
- 유연성
- 부정적 영향을 막기 위해서는 구체적 기준이나 보충이 필요함. 국내 입법 가능하게, 아예 명시하거나, 기타 방안. 각기 장단점 있음.

다. 처리 반대와 관련하여(right to object)

- 적법한 이해 평가. direct marketing인 경우는 평가 허용되지 않음

라. .9조와의 관계

- 중첩적용 vs 특별관계
- 9조의 요건이 완화된 경우도 있으므로 중첩적용되어야 한다.

3. 두 가지 테스트

가. 필요성(necessity test)

- Consent 외의 5가지 요건은 모두 필요성 평가가 필요함 : 필요한 범위
- 공동체 법률에서 독립적 의미를 갖는 요건임(ECJ, Heinz Huber), ECtHR(필수불가결한과는 다른 의미이지만, 합리적인, 바람직한, 통상의, 유용한, 허용되는 등과 같은 유연한 용어와도 다르다고 함)
- 다른 원칙 – 공정, 적법, 필요, 비례, 정확성 등 준수

나. 균형(balancing test)

- Legitimate interest 외에 다른 조항에서도 요구함.
- 맥락 속에서 평가되어야 하기 때문에 필수적 요건이기도 함.

4. 이해(interest)

가. 목적과 연관되지만 다름

- 목적은 데이터가 처리되는 특별한 이유. 정보 처리의 목표이나 의도.
- 이해관계는 처리자가 처리 과정에서 가질 수 있는 더 넓은 stake, 처리자가 그 처리로부터, 또는 사회가 처리로부터 얻게 되는 혜택
- 예를 들어 원자력 발전소에서 회사는 일하는 직원들의 건강과 안전을 보장할 이해가 있다.
- 이 경우 회사는 직원의 건강과 안전을 보장하기 위해 특정 개인정보의 처리에 대하여 접근 통제 조치 절차를 이행할 목적이 있을 수 있고, 그에 따라 특정한 개인정보의 처리를 정당화할 수 있음.

나. Legitimate interest

- 법률상 수용 가능해야 함

- 이익형량이 가능할 수 있을만큼 합법적이고, 충분히 명확하고, 분명해야 함
- 실제적이고, 현재의 것이어야 함
- 합법적 이해가 있다고 해서 이 요건이 적용될 수 있는 것은 아님. 출발점임.
- 프로파일링의 사례
- 공공부문의 경우 : 이 요건과 public task에 대한 요건의 관계. Public task의 경우는 법률에 의해 적절한 승인이 있어야 함. 상세하고 특정되어야 함.

다. 제3자의 적법한 이해

- 예를 들어 투명성과 책임성 확보하기 위한 목적으로
- 이익형량이 필요함.
- 적절한 보호 수단
- 역사적, 과학적 연구
- 일반적 공익

라. 필요성 요건

5. 정보주체의 권리나 이익

가. 권리나 이익은 넓게 해석해야 함

나. 권리나 이익

- 사생활, 익명의 권리 보호할 필요 커짐 : 정보의 집적, 불균형
- 정보주체의 경우 'legitimate' interest가 아닌 'interest'임.

6. 이익형량

가. 보호조치 중요

나. 사례 분석

(1) 피자 체인의 특별 서비스

모바일 앱으로 피자를 주문한 사람에게 며칠 후 피자 체인에서 주문시 주소를 활용하여 주문자에게 비슷한 제품의 할인 쿠폰 우송

- 피자 체인의 정당한 이익
- 주문자의 권리나 이익
- 보호 조치
- 이익형량

(2) 피자 체인의 타겟 마케팅

모바일 앱으로 피자를 주문한 사람에게 며칠 후 피자 체인에서 주문시 주소를 활용하여 주문자에게 주문 내역과 피자 체인에서 운영하는 슈퍼마켓 이용내역(온라인, 오프라인), 위치 정보 등을 제공받아, 이를 분석하여 특정 할인 등 타겟 광고를 실시함. 해당 회사는 할인 조건이나 알고리즘을 알려주지 않음.

- 피자 체인의 정당한 이익
- 주문자의 권리나 이익
- 보호 조치
- 이익형량

(3) 음식 주문 내역을 보험 회사에 제공

피자.소비 습관과 시간 등을 보험 회사에 판매, 보험회사는 이를 건강보험 요율에 적용

- 피자 체인의 정당한 이익
- 주문자의 권리나 이익
- 보호 조치
- 이익형량

다. 이익형량시 고려할 요소

- 처리자의 합법적 이익
- 정보주체에게 미치는 영향
- 개인정보 보호에 관한 법률상 의무사항를 준수하는지 여부
- 개인정보에 대한 추가적 보호조치

라. 처리자의 합법적 이익

(1) 기본권의 행사

- 기본권의 충돌시 형량
- 필요성과 비례 원칙

(2) 공익, 공동체의 이익
(3) 기타 합법적 이익
(4) 합법적 이익에 대한 사회적, 문화적 인식도 고려

마. 정보주체에게 미치는 영향

(1) 영향의 평가
(2) 개인정보의 성질
(3) 개인정보 처리 방법
(4) 정보주체가 합리적으로 예측할 수 있는지
(5) 정보처리자와 정보주체의 지위

바. 개인정보 보호에 관한 법률상 의무사항을 준수하는지 여부

사. 개인정보에 대한 추가적 보호조치

7. 책임성과 투명성 – 부가적으로 적용됨.

8. 거부할 권리

가. Public task(6(e))의 경우와 legitimate interest(6(f)), 프로파일링(22)의 경우

나. 'compelling legitimate ground'

- Directive 95/46에서는 거부할 권리 행사의 요건으로 정보주체에게 compelling legitimate ground를 설명할 수 있어야 한다는 규정이 있었음. 정보주체가 이를 입증해야 했음(14(a)). 단 원격 마케팅은 이런 요건 필요 없도록 함(14(b)).
- GDPR은 거꾸로 정보처리자가 이를 입증해야만 계속 처리가 가능하도록 함. 따라서 입증 책임도 전환(21(1)).

9. 원격 마케팅(direct marketing)에 적용

가. 유럽연합의 규정

(1) ePrivacy Directive (13조)
- 기존 고객에 대해 유사 상품의 광고는 opt out
- 그 외 이메일 마케팅과 자동 발신 전화 마케팅은 사전 동의 필요

(2) Directive 95/46(14(b))
- 원격 마케팅 거부할 권리 보장

나. 원격 마케팅에 대한 규율

(1) 기존 고객 유사상품 광고 : 동의 필요 없이 (GDPR 7(f)). 그러나 무조건 Opt out 보장
(2) 이메일 마케팅, 자동 발신 전화 마케팅 : 사전 동의 필요(GDPR 7(a)).
(3) 행태 분석에 따른 광고, 타겟 마케팅 : 사전 동의 필요