중국 개인정보보호법의 이해

Contents

What is 개인정보?

- **전자 또는 다른 방식으로 기록**되어 **단독 또는 기타 정보와 결합**하여 **자연인의 개인 신분을 식별**할 수 있는 각종 정보(중국 네트워크안전법 제76조 5)

- 전자 또는 기타 방식으로 기록되고, **이미 식별되거나 식별 가능한** 자연인 관련 모든 정보 단, 익명 처리 이후의 정보는 포함되지 않음(중국 개인정보보호법 제4조)

- "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보 (한국 개인정보보호법 제2조1)

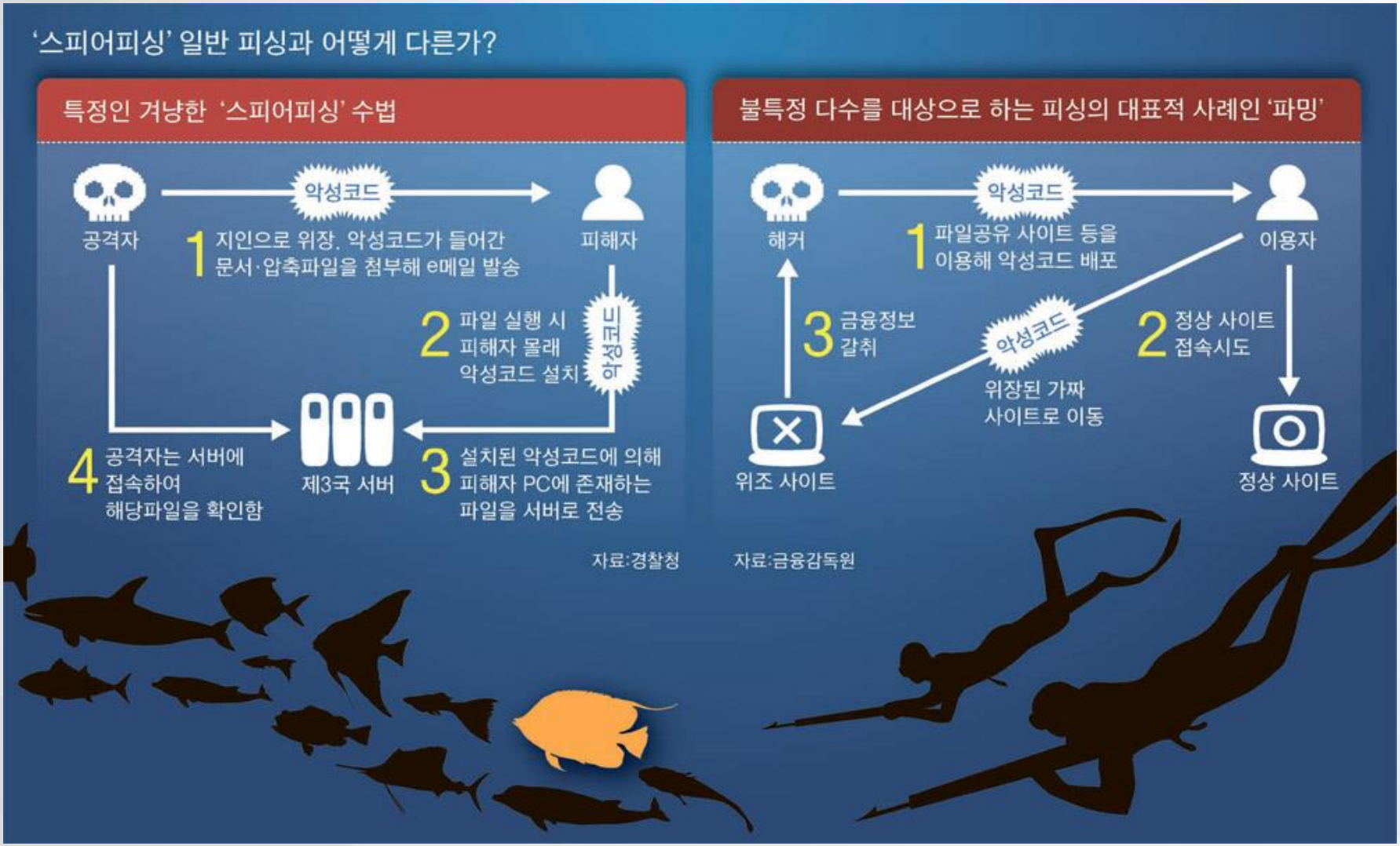
가. **성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보**

나. **해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보.** 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.

다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "**가명정보**"라 한다)

1. 들어가며 – 개인정보 사고유형 (1)

- 무심코 누른 e메일 첨부파일 · · · 특정 대상을 노리는 APT 공격 '스피어피싱'

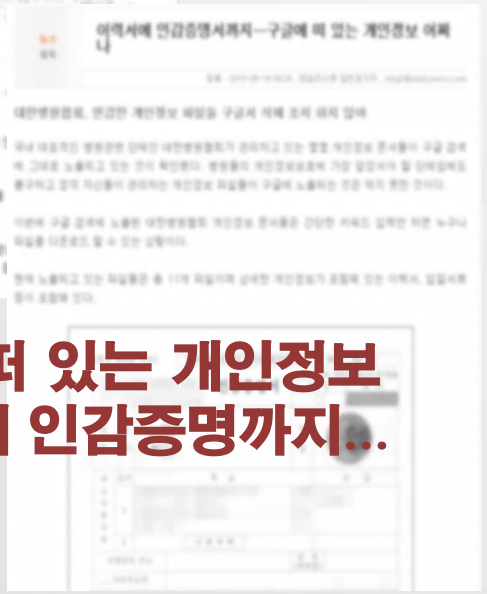


< 그림 출처 : 인터넷 >

1. 들어가며 – 개인정보 사고유형 (2)

OO기관 채용지원자
개인정보 유출

XX보험사 고객정보 70만건
인터넷에 노출

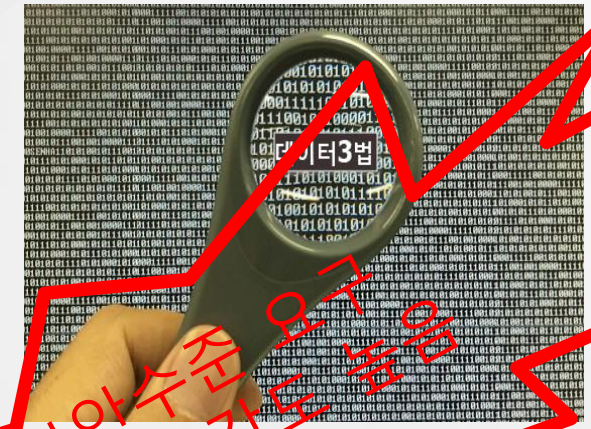


구글에 떠 있는 개인정보
이력서에 인감증명까지...

구글 검색에 취약한
웹 페이지들...

1. 들어가며 – 주요국 개인정보보호 관련 제도

< EU GDPR >



< 한국 데이터3법 >

< APEC CBPR >

높은 보안수준 요구
위반시, 제재 가능성 증가

< 캘리포니아주
소비자 프라이버시 보호법>

< 베트남 사이버보안법 >

< 인도 개인정보보호법>

그림 출처 : 인터넷

1. 들어가며 – 중국 개인정보 관련 제도

네트워크안전법(17.6월 시행)

- 제4장 네트워크정보보호(제 40조~45조)

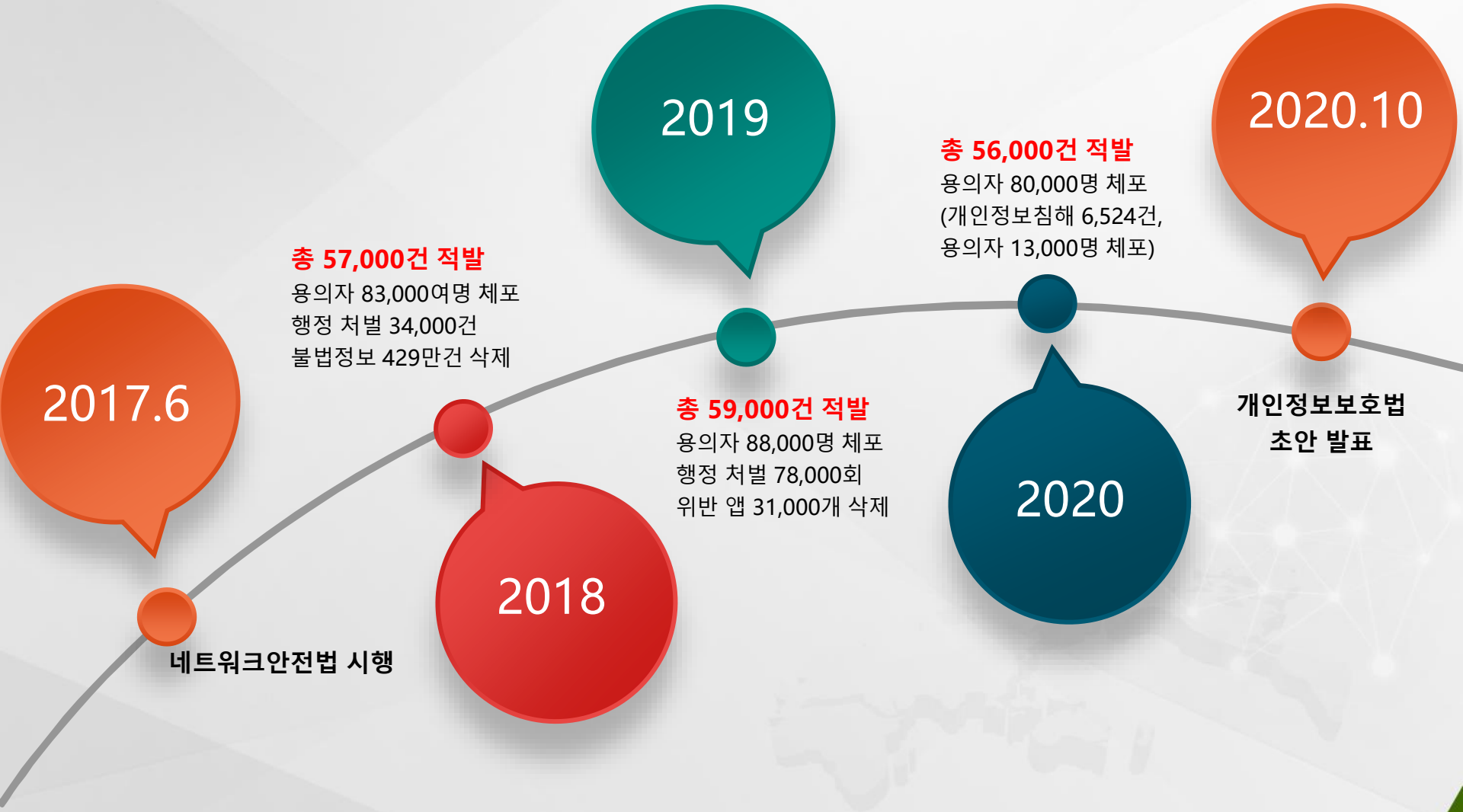
민법전(21.1월 시행)

- 제4편의 제6장(사생활권과 개인정보보보호)

개인정보보호법(초안)

- 총 8장 70조로 구성
  [개인정보 영향평가 지침(6월 시행)]
  [모바일 인터넷 앱의 필수 개인정보 범위 규정(5월 시행]

1. 들어가며 – 중국 단속 현황(징왕, 净网)



2. 중국 개인정보보호법(초안) – 적용 대상

- 기관, 개인이 **중화인민공화국내에서 자연인의 개인정보를 처리하는 경우**
- **국외**에서 개인정보 처리 時, 아래에 해당되는 경우

(1) 국내 자연인에게 상품 또는 서비스를 제공하는 목적

(2) 국내 자연인의 행위를 분석, 평가

(3) 법률 및 행정법규에 규정된 기타 사항

개인정보

전자 또는 기타 방식으로 기록되고,
이미 식별되거나 식별 가능한
자연인 관련 모든 정보

익명 처리 이후의 정보는 포함되지 않음

2. 중국 개인정보보호법(초안) – 개인정보 Life Cycle

2. 중국 개인정보보호법(초안) – 수집 (1)

▪ **개인정보 처리 조건**

(1) 개인의 동의를 받은 경우

(2) 계약의 수립 또는 이행에 필요한 경우

(3) 법적 직무 또는 법적 의무의 이행을 위해 필요한 경우

(4) 공공보건사고에 대응하거나, 응급한 상황에서 자연인의 생명 건강 및 자산 안전보호를 위해 필요한 경우

(5) 공공의 이익을 위한 신문 보도, 여론 모니터링 등 합리적인 범위 내에서 개인정보를 처리하는 경우

(6) 법률, 행정법규에서 규정하는 기타 상황

▪ 개인의 동의를 기반으로 **민감 개인정보*를 처리하는 경우, 별도 동의**

(개인에게 민감 개인정보 처리 필요성 및 개인에게 미치는 영향 고지)

* 종족, 민족, 종교 신앙, 개인 생물 특징, 의료 건강, 금융 계좌, 개인 행적 등

▪ **만 14세 미만 미성년자의 개인정보**라는 사실을 알거나 알아야 하는 경우,

보호자의 동의를 받아야 한다.

2. 중국 개인정보보호법(초안) – 수집 (2)

- (네크워크안전법 제41조) 네트워크운영자는 **그가 제공하는 서비스와 무관한 개인정보를 수집해서는 아니 되며** 법률, 행정법규의 규정과 쌍방의 약정을 어기면서 개인정보를 수집 및 사용해서는 아니된다.
- (모바일 앱 규정 제3조, 4조) **필수/선택 개인정보로 구분하여 동의를 받고**, 선택 개인정보의 경우 동의를 하지 않는다고 기본기능 서비스를 거부해서는 안 됨

구분	필수 개인정보
지도 네비게이션	위치정보, 출발지, 도착지
인터넷 예약 차량	1. 가입 이용자의 휴대전화 번호 2. 승차자의 출발지, 도착지, 위치정보, 행적 3. 결제 시간, 결제 금액, 결제 방식 등 결제 정보
학습, 교육	가입자의 휴대전화 번호
인터넷 결재	1. 가입 이용자의 휴대전화 번호 2. 가입 이용자의 성명, 증명서 유형 및 번호, 증명서 유효기간, 은행카드번호
인터넷 구매	1. 가입 이용자의 휴대전화 번호 2. 수취인의 성명(이름), 주소, 연락처 3. 결제 시간, 결제 금액, 결제 방식 등 결제 정보
외식 배달	1. 가입 이용자의 휴대전화 번호 2. 수취인의 성명(명칭), 주소, 연락처 3. 결제 시간, 결제 금액, 결제 방식 등 결제 정보
운동, 헬스	-

< 앱의 필수 개인정보(예) >

2. 중국 개인정보보호법(초안) – 수집 (3)

01 개인정보처리자 신분, 연락처

02 처리 목적, 방식, 개인정보 유형, 보관 기간

03 개인 권리 행사 방식, 절차

04 법에서 정한 고지 사항

☞ 사전에 분명한 방식과 명확하며 알기 쉬운 언어로 고지,

☞ 변경이 발생할 경우 변경된 부분을 고지

2. 중국 개인정보보호법(초안) – 보관/이용

▪ 업무 상 필요로 해외로 개인정보를 제공하는 경우, 다음 중 한가지 이상 충족

(개인정보를 제공받는 자의 신분, 연락처, 처리 목적, 처리 방식, 개인정보 유형, 권리행사 방법 등을 **고지하고 별도 동의**)

(1) 안전성 평가 통과

(2) 전문기관의 개인정보 보호 인증 수행

(3) 해외에서 개인정보를 이전받는 자와 계약을 체결하고, 양측의 권리와 의무를 약정하며, 개인정보 처리행위가 본 법률과 부합하는지 감독

(4) 법률, 행정법규 또는 국가 네트워크 정보 부처에서 규정한 기타 조건

▪ 핵심정보 인프라 운영자와 개인정보 처리규모가 국가 네트워크 정보 부처에서 규정한 기준에 해당하는 개인정보처리자의 경우,

- **국내에서 생성된 개인정보를 국내에 보관**
- **해외 제공 시, 국가 네트워크 정보 부처 기관의 안전성 평가를 통과해야 함**

2. 중국 개인정보보호법(초안) – 이용(위탁/3자 제공)

▪ (제22조) 개인정보처리자가 개인정보 처리를 위탁하는 경우, 수탁 처리의 목적, 방식, 개인정보 유형, 보호 조치 및 양측의 권리 의무 등을 수탁자와 약정해야 하며, 수탁자의 개인정보 처리 행위에 대하여 감독을 실시해야 한다.

▪ (제24조) 개인정보처리자가 제3자에게 처리한 개인정보를 제공하는 경우, **개인에게 제3자의 신분, 연락처, 처리 목적, 처리 방식 및 개인정보 유형을 고지하고 개인으로부터 별도의 동의**를 받아야 한다.
개인정보를 이전 받은 제3자는 위에서 언급한 처리 목적, 처리 방식 및 개인정보 유형 등 범위 내에서 개인정보를 처리해야 한다. **제3자가 기존의 처리 목적, 처리 방식을 변경하는 경우 본 법의 규정에 근거하여 개인에게 다시 고지하고 동의**를 받아야 한다.

2. 중국 개인정보보호법(초안) – 개인정보처리자 의무 (1)

▪ (제50조) 개인정보 처리 행위가 법률, 행정법규 규정에 부합되도록 보장하고, 비인가자에 의한 접근 및 개인정보 유출 등을 예방해야 함

(1) 내부관리제도 및 운영규정 마련

(2) 개인정보를 등급별로 구분하여 관리

(3) 암호화, 비식별화 등 상응하는 보안 기술 조치 적용

(4) 개인정보 처리 운영 권한을 합리적으로 확정하고, 종사자에 대한 보안 교육 및 훈련 실시

(5) 개인정보 보안사고 응급방안을 수립하고 실시

(6) 법률, 행정법규에서 규정한 기타 조치 수행

▪ (제51조) 개인정보 처리규모가 국가 네트워크 정보 부처에서 규정한 일정 기준에 해당 되는 **개인정보처리자는 개인정보 보호 책임자 지정**

▪ (제52조) 국외 개인정보처리자는 **중화인민공화국 국내에 전문 기관을 설립하거나, 대표자를 지정**

- 유관기관 명칭 또는 대표자 성명, 연락처 등을 담당부처에 보고

2. 중국 개인정보보호법(초안) – 개인정보처리자 의무 (2)

▪ (제54조) 개인정보처리자는 아래의 개인정보 처리 행위에 대해 **사전에 리스크 평가**를 실시하고 처리 상황을 기록해야 한다.

(1) 민감 개인정보 처리

(2) 개인정보를 이용한 자동 의사 결정

(3) 개인정보 처리 위탁, 제3자에게 개인정보 제공, 개인정보 공개

(4) 개인정보 국외 이전

(5) 개인에게 중대한 영향을 미치는 기타 개인정보 처리 행위

개인정보 영향평가

개인정보 처리활동의 합법성과 컴플라이언스를 검사하여 개인정보 주체의 합법적 권익을 침해하는 각종 위험을 판단하고, 개인정보 주체를 보호하기 위한 각종 조치의 유효성을 평가하는 과정

[첨부] 개인정보 영향평가 Process

1 평가 필요성 분석

2 평가 준비
(평가팀 구성→평가계획 수립→평가대상과 범위 확정→자문계획 수립)

3 데이터 매핑 분석
(데이터 리스트 및 데이터 Flow Chart 작성)

4 위험원 식별
(1) 네트워크 환경 및 기술적 조치 (2) 개인정보 처리절차 (3)평가 대상 및 제3자 (4) 업무 특징, 규모 및 보안현황

5 개인 권익 영향분석
(1) 개인의 자율성 제한 (2) 차별대우 유발 (3) 개인의 명예훼손 또는 정신적 스트레스 (4) 인명과 재산 손실

6 보안위협 종합분석

2. 중국 개인정보보호법(초안) – 벌칙

■ 개인정보 불법 처리 또는 처리 시 보안조치 미흡 時,

☞ 백만 위안 이하의 벌금

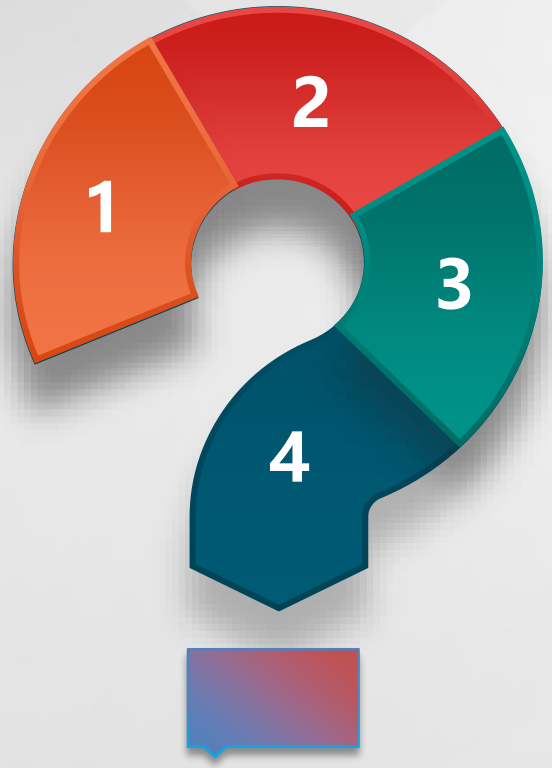
☞ 사인이 심각할 경우, 5천만 위안 이하 또는 전년도 매출액의 5% 이하에 해당하는 벌금형

■ 이용자 권익 침해 時,

☞ 개인의 손실 또는 개인정보처리자의 이익에 근거하여 배상

그림 출처 : 인터넷

마치며



1 **개인정보 범위**
생각보다 광범위

2 **개인정보 수집 時**
동의 받자, 잘 받자!!

3 **법 위반 時**
개별 소송 및 행정/사법기관 조사로 고생
처벌 수위가 높다!

4 **준비하자**
시간이 부족하다

Internet On, Security In!

감사합니다