CPPG 출제범위내의 용어정리 및 해설

개인정보보호법령,정보통신망법령의 각지침및고시/비식별/GDPR 등 CPPG 범위내의 용어 정의 정리

작성자 :ERIC_YOON
YOONSWEETY.ERIC@GMAIL.COM

이런 마음으로 정리해 보았습니다.

CPPG 시험을 준비하다보니 각 법령에 따른 고시,지침등 수많은 자료를 봐야만합니다.

- 수없이 읽고 읽다보면 중복으로 나오는 용어 정의 반복들....
- 각용어의 정의는 매우 중요합니다 .

  예를들어 내손가락을 법령에서 컵이라고 정의한다면 그순간 내손가락은 컵이 되는것이다.
- 확실하지 않은 어렴풋한 짐작으로 정의를 내리면 이시험을 준비하는 내내 고생을 할수 밖에 없는 어리석은 방법이다.
- 이자료...저자료... 정리도 안되고...범위도해석도 다르고...
- 그래서 정리를 좋아하는 필자는 수험자의 입장에서 굳이 정리를해보며 복습도하면서 정리해 보았습니다.
- 제일먼저 이자료를 보시고 각 법령 지침 을 보시기 바랍니다.
- 이 용어정의를 확실히 정리하신후에 지침,고시에 용어정의가 나오면 과감히 패스를 하여 시간을 절약 하실수 있으실거라 생각합니다.
- 범위는 개보법령,망법,의 각지침및고시와 비식별,GDPR 까지 이며 중간중간 지극히 주관적인 필자의 생각을담아보았습니다. 필자의 경우 그런의미로 암기를하고 머리속에 집어넣었기때문에

  굳이 그런정보는 참고만해주시길 바랍니다.

많이 부족한 자료 이지만, 나름대로 열심히 공부 하였고, 지금 이시간에도 열심히 공부할 누군가와 공유 하고 싶어 작성 하게 되었습니다.

감사합니다 ^^

작성자: Eric Yoon / yoonsweety.eric@gmail.com

CPPG 출제범위내의 용어정리 및 해설

법령 많이 보게 되는데 왠만해서는 3 단 비교로 보길 바랍니다.

처음 몸을비비꼬시며 보시더라도 끝까지 한번 보시고 , 다시 또 보시기 바랍니다.

읽고 뒤돌아서면 도통 무슨말인지 기억도 안나던 부분이 본인도 모르게 머리에 박혀 있을겁니다

여러분은 엄청 똑똑하시 잖아요 ^^!

법의 구성은

헌법>법률>시행령>시행규칙>조례>고시

하위부분일수록 세분화 되어 있다는점!

법률

국회의 의결을 거쳐 대통령이 서명하고 공포함으로써 성립하는 국법

시행령 = 대통령령

어떤 법률을 시행하는 데 필요한 규정을 주요 내용으로 하는 명령. 일반적으로 대통령령 으로 제정

시행규칙

법령의 시행에 관한 사항을 상세히 규정한 규칙. 일반적으로 대통령령의 시행에 관하여 필요한 사항을규정한 총리령 또는 부령(部令) 따위를 이른다.

고시

행정 기관이 일반 국민들에게 글로 써서 게시하여널리 알림. 주로 행정기관에서 일반 국민들을 대상으로 어떤 내용을 알리는 경우를 이른다.

작성자: Eric Yoon / yoonsweety.eric@gmail.com

개인정보

개인정보보호법과 정보통신망법은 법률상 표현이 다르지만, 내용은 사실상 같다.
각 법률의 차이를 익히자!!! 개보법은 서류도 포함 . 정통망법은 서류 는 포함이 아니다 !!

개인정보보호법 제 2 조 1 호

-살아있는 개인에 관한 정보로서 성명,주민등록번호및영상 등을 통해 개인을 알아볼수있는정보 (해당정보만으로 특정 개인을 알아볼수 없더라도 다른정보와 쉽게 결합하여 알아볼수 있는 것)

정보통신망법 제 2 조 1 항 6 호

-생존하는 개인에 관한 정보로서 성명,주민등록번호 등에 의하여 특정한 개인을 알아볼수 있는 부호,문자,음성,음향,영상 등의 정보(해당정보만으로 특정개인을 알아볼수 없어도 다른 정보와 쉽게 결합하여 알아볼수 있는 정보)

정보주체

처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

정보의 주체가 되는 사람 의미

개인정보파일

개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

일정한 규칙은 반드시 이름,주소,연락처등 오름차순이나 내림차순으로 정렬된 것뿐이 아니라 개인정보파일에 포함된 개인정보 항목의 검색을 가능하게 하는 규칙 존재한다면 , 이또한 일정한규칙의 범주에 포함된다.

또한, 반드시 개인정보 파일이 전자기적으로 배열된 데이터를 의미하지 않다!!!

개인정보보호법에서는 수기로된 문서도 개인정보로 정의 하고 있다.

작성자: Eric Yoon / yoonsweety.eric@gmail.com

개인정보 처리

개인정보를 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

개인정보처리자

법 제 2 조제 5 호에 따른 개인정보를 처리하는 모든 공공기관, 영리목적의 사업자, 협회·동창회 등 비영리기관·단체, 개인 등을 말한다.

개인정보처리자의 개인정보 보유량에 따라 3 가지 유형으로 구분하여 각각 안전조치 의무 기준을 규정 하고 있다.

유형	적용대상
유형 1(완화)	- 1 만명 미만의 정보주체에 관한 개인정보를 보유한 소상공인,단체,개인
유형 2(표준)	- 100 만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업 - 10 만명 미만의 정보주체에 관한 개인정보를 보유한 대기업,중견기업,공공기관 - 1 만명 이상의 정보주체에 관한 개인정보를 보유한 소상공인,단체,개인
유형 3(강화)	- 10 만명 이상의 정보 주체에 관한 개인정보를 보유한 대기업,중견기업,공공기관 - 100 만명 이상의 정보주체에 관한 개인정보를 보유한 중소기업,단체

비영리 목적 이라할지라도 업무에 해당 된다면 개인정보 처리자 로 봐야한다 !!!!

작성자: Eric Yoon / yoonsweety.eric@gmail.com

공공기관

제 2 조제 6 호 및 「개인정보 보호법 시행령」(이하 "시행령"이라 한다) 제 2 조에 따른 기관을 말한다.

대기업

「독점규제 및 공정거래에 관한 법률」제 14 조에 따라 공정거래위원회가 지정한 기업 집단을 말한다.

중견기업

「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」제 2 조에 해당하는 기업을 말한다.

중소기업

「중소기업기본법」제 2 조 및 동법 시행령 제 3 조에 해당하는 기업을 말한다.

5~50 명

10~50 명 (건설업,제조업,운수업,광업)

소상공인

「소상공인 보호 및 지원에 관한 법률」제 2 조에 해당하는 자를 말한다.

상시종업원수가 5 인 이하 = ~4 인 미만

상시종업원수가 10 인 이하 = 1~9 인 미만인 (건설업,제조업,운수업,광업)

인터넷 정보통신업체 = 전년도말 직전 3 개월간 일일평균 이용자 1 천명 이하

작성자: Eric Yoon / yoonsweety.eric@gmail.com

개인정보 보호책임자 CPO

개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영

제 32 조제 2 항에 해당하는 자를 말한다.

정보통신망법의 개인정보책임자도 의미가 같다

정보통신서비스제공자의사업장내에서이용자의
개인정보보호 업무를 총괄하거나 업무처리를 최종 결정하는 임직원을 말한다.기존부서의 장이 겸임할수 있다. 이때 공식으로 지정하여 관련 서류를 구비하도록 하고 , 내부계획의 수립을 참고하여 각 책임역활을 분명히 하여야 한다

개인정보취급자

개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원,

파견근로자, 시간제근로자 등을 말한다.

방송통신위원회 고시에서 개인정보 취급자는 이용자의 개인정보를

수집,보관,처리,이용,제공,관리, 또는 파기 등의 업무를 하는자 라고 규정하고 있다.

개인정보처리시스템

데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.

DBMS 이다.

공개된 무선망

불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

흔히 공항,커피숍,도서관 등 공개 와이파이로 접속가능한 무선접속장치이다.

업무를 목적으로한 CDMA,WCDMA 등의 기술을 사용하는 이동통신망은 공개된 무선망은

아니다 !!

작성자: Eric Yoon / yoonsweety.eric@gmail.com

정보통신망

「전기통신기본법」 제 2 조제 2 호에 따른 전기통신설비를 이용하거나 전기통신 설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.

간단하게 정보통신 설비를 이용하여 전기통신 설비와 컴퓨터 및 컴퓨터 이용기술을 활용하여 정보를 수집,가공,저장,검색,송신 수신하는 정보통신 체계를 의미한다.

위험도 분석

개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험 요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.

개인정보 유출상황을 가정해서 침해가능성 및 피해의 정도를 가늠해보는 것으로 민감도분석,시나리오작성 등 정량적분석방법과 정성적 분석 방법을 상황에 맞게 적절하게 판단하여 분석 할수 있다.

ㅇ 위험도 산출

- 서비스별 영향도, 발생가능성을 고려해서 위험도를 산출할 수 있다.

- 서비스별 개인정보 영향도 산출공식(예) = $A\frac{1}{n}\left(\sum_{i=1}^{n} B_i(1-C_i)\right)$

  A: 서비스별 고객정보 중요도

  B : 점검항목별 위험 심각도

  C : 점검항목별 보호대책 이행 수준

  n : 서비스별 총 점검항목 수

- 이때, 수치가 클수록 위험이 심각하다는 것을 의미한다.
  또한 이는 Risk Matrix를 통해서도 대응방안에 대한 전략 수립이 가능하다.

작성자: Eric Yoon / yoonsweety.eric@gmail.com

식별자

ID/계정을 뜻함.

모바일 기기

무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿 PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.

비밀번호

정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보 통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

비밀번호를 분실하였다 하더라도 고객센터등 서비스이용자의 편의를 위해 앞자리라도 알려주는 것은 위법이다 !!!

비밀번호는 반드시 암호화 알고리즘 SHA128 비트 이상

일방향 해쉬 처리하여 보관하여야 한다.

(숫자-10, 알파벳대-26. 소문자-26, 특수문자-32

= 조합중 2 개 이상의 조합일경우 10 자리 설정 !

= 조합중 3 개 이상의 조합일경우 8 자리 설정 !)

권고 사항 아님 !!! 비밀번호 유효기간은 반기별 1 회 이상 !!

작성자: Eric Yoon / yoonsweety.eric@gmail.com

모바일 기기

무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿 PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.

바이오정보

지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

신체적특징-지문,필적,외형,망막 등 ,

행동적특징-필적,걸음걸이,키보드타이핑속도와 손가락 높이등...으로 구분할수 있다.

이런 신체적특징,행동적특징을 기술적 방법으로 수집후 가공하지 않은 원본상태로 보존하는 원본정보와, 특정 알고리즘을 통해 특정만을 추출 가공하여 생성한 특정정보 로 구분된다.

유전자-DNA 를 이용한 개인식별은 개별법인 [생명윤리 및 안전에 관한 법률을 적용한다]

보조저장매체

이동형 하드디스크, USB 메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.

보조기억장치 가 아니다 !!!

반드시 용이하게 분리될수 있어야 한다 !!

컴퓨터 본체 케이스를 오픈하였다고 해서 하드디스크를 쉽게 분리할 수는 없다 =보조기억장치는 맞지만 보조저장매체는 아니다. (필자는 이부분 용어정리가 안되서 한참 이해가 안되었었다. 머리가 나쁜가보다....)

USB,IEEE1394 등 표준인터페이스를 통해 탈착이 용이한 매체이다.

작성자: Eric Yoon / yoonsweety.eric@gmail.com

내부망

물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

접속기록

개인정보취급자 등이 개인정보처리시스템에 접속한 사실을 알 수 있는 계정, 접속일시, 접속자 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리 시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.

게정,접속일시,접속자,수행업무를 알수 있는정보는 일반적으로 개인정보 처리시스템에 접속한 당사자의 ID,접속시간,IP 주소를 의미. 이런정보는 로그기록이라 불린다. 이러한 정보는 수기로 기록되서는 안되며 실시간으로 전자적,자동적으로 기록 되어야 하며 위,변조 되지 않도록 관리를해서 차후에 책임추적성으로 대응가능하도록 관리에 주의를 기울여야한다.

📂 업무를 수행한 기록 이다.
예) 이용자= 본인의 개인정보 수정,탈퇴,등등
처리자= 수집,보관,관리,파기등
이러한 기록을 시스템에 의해 자동적으로 생성된 전자적 기록 !!!!!
(수기기록은 접소기록으로 부적절하지만 환경에 따라 책임자의 확인절차에 따라 가능도 하다.대체적으로 부적절하다 전자적 기록 으로 각인을 해놓자)

친목단체

학교, 지역, 기업, 인터넷 커뮤니티 등을 단위로 구성되는 것으로서 자원봉사, 취미, 정치, 종교 등 공통의 관심사나 목표를 가진 사람간의 친목도모를 위한 각종 동창회, 동호회, 향우회, 반상회 및 동아리 등의 모임을 말한다.

(비영리 목적이므로 반드시 개인정보 책임자를 지정 하지 않아도 된다. 제외대상 .

하지만 업무로 보는 시각도 있기에 취급자는 각 대표가 수행하는 것이 적절하다)

작성자: Eric Yoon / yoonsweety.eric@gmail.com

관리용 단말기

개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말한다.

개인정보처리시스템 DBMS 에 직접 접속하는 관리자의 PC,노트북 등을 의미.

관리용단말기에는 침해사고 방지를 위하여 안전조치를 취하여야한다

(제 10 조 관리용단말기의 안전조치)

- 인가 받지않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
- 본래 목적 외로 사용되지 않도록 조치
- 악성프로그램 감염 방지 등을 위한 보안조치 적용

영상정보처리기기

일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치로서 시행령 제 3 조에 따른 폐쇄회로텔레비전(CCTV) 및 네트워크카메라를 말한다.

개인영상정보

영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등 사생활과 관련된 영상으로서 해당 개인의 동일성 여부를 식별할 수 있는 정보를 말한다.

영상정보처리기기 운영자

개인정보 보호법 제 25 조제 1 항 각호에 따라 영상정보처리기기를 설치·운영하는 자를 말한다.

작성자: Eric Yoon / yoonsweety.eric@gmail.com

공개된 장소

공원, 도로, 지하철, 상가 내부, 주차장 등 정보주체가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 말한다.

P2P(Peer to Peer)

정보통신망을통해서버의도움없이개인과개인이
직접 연결되어 파일을 공유하는 것을 말한다.
꼭 전문적인 p2p 가 아닌, 인스턴트메시지, 웹하드등 , 서버를 거치지 않고
당사자간의 통신만으로 파일을 전송하는 것을 통칭함.

공유설정

컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을
할 수 있도록 설정하는 것을 말한다.

보안서버

정보통신망에서 송·수신하는 정보를 암호화하여 전송하는
웹서버를 말한다.
SSL 인증서/HTTPS 를 통해 암호화된 통신을 하는 웹서버를 지칭

인증정보

개인정보처리시스템또는정보통신망을관리하는시스템등이
요구한 식별자의 신원을 검증하는데 사용되는 정보를 말한다.
신원을 검증하는데 사용되는 정보로써-비밀번호,바이오정보,전자서명값을말한다.

정보통신서비스제공자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보 처리시스템에 접속이 필요한 경우에는 공인인증서등 안전한 인증수단을 적용해야한다.
-외부에서 접속시 단순 비밀번호는 불충분할수 있음.
-그사람이 가지고 있는 것 - what You Have = 공인인증서등등..
-그사람이 알고있는 내용 - What You Have = 비밀번호..고향...학교교수님.
-보안토큰,휴대폰인증,일회용비밀번호(OTP,바이오정보,단말기 IP)등 고려.

작성자: Eric Yoon / yoonsweety.eric@gmail.com

그 외 기본 베이스 용어

동의

정보주체와 개별적으로 연락을 하여야 하고 반드시 정보주체로부터 피드백을 받아야 한다.

통지,고지

정보주체와 개별적으로 연락은 해야하지만 , 피드백을 받을 필요는 없다.

정보주체에게 알려야한다는것에 포커스를 두고 있으므로, 전달은 확실히 해야한다

단 피드백을 받을 필요는 없기에 동의와 구분된다.

안내,공지,게시

정보주체와 개별적으로 연락할 필요도 없고, 당연 피드백을 받을 필요도 없습니다.

웹사이트의 공지사항이나, 갈음방법중 한방법이 될수도 있고 , 정기간행물,신문 등

정보주체가 서비스를 이용하면서 쉽게 확인할수 있는 것 !!

지체없이..

개인정보처리자가 정보주체의 요구에대해 조치를 가장 우선순위를 두어 처리하는데 소요되는 시간 으로써, 개인정보처리자가 고의로 업무처리를 지연한 사정이 없다고 보이는 이상에는 지체없이 필요한 조치를 취했다 라고 할수 있다.

단, 지체없이 의 기간 이 일률적으로 정하기 곤란하기에 정보주체의 요구사항과 개인정보처리자의 업무트성을 종합하여 합리적이였는지로 판단 할수 있다.

(개인정보보호법 중 4 장 정보주체 권리 까지는 5 일로 보고 5 장 정보주체 권리 부분부터는 10 일로 보는 것이 암기에 도움이된다)

작성자: Eric Yoon / yoonsweety.eric@gmail.com

갈음

말그대로 갈아치워서 한다 는 의미입니다.

다른 것으로 바꾸어 대신함.

보통 통지에 대해 갈음 하는 방법이 많이 나옵니다. 몇가지안되니 암기하세요

당해 제공자,이용자..

바로 그 사물에 해당됨을 나타내는 말 로,

현재 재직중이거나 , 현재 서비스를 제공 받는자 등 의 의미로 파악 하길 바란다.

쉽게 결합하여

결합 대상이 될 정보의 입수 가능성이 있어야 하고, 결합 가능성이 높아야 함을 의미

-입수가능성 = 두종이상의 정보를 결합하기 위해ㅐ서 결합에 필요한 정보에 합법적으로 접근, 입수할수 있어야 함. 불법적인 정보는 아님.

-결합가능성 = 합법적인 방법으로 정보를 입수하여 현재의 기술 수준에 비추어 결합이 사실상 불가능 하거나 결합하는데 비합리적인 수준의 비용이나 노력이 수반된다면 이는 결합이 용이하다고 할수 없다.

작성자: Eric Yoon / yoonsweety.eric@gmail.com

전기통신 사업자 1

전기통신사업자는 [전기통신사업법]의 규정에 따른 허가,등록,신고 절차를 거친 기간통신 사업자,별정통신사업자,부가통신 사업자를 말한다.

기간통신 사업자

초고속 인터넷기업,이동통신사 등 유,무선 통신 사업자로서

직접 회선설비를 설치하고 주파수를 할당받아 통신서비스를제공하는 사업자.

방송통신위원회의 허가를 얻은사업자이다.

흔히 우리가 아는 SK,KT 등 .....

별정통신사업자

기간통신사업자의 전기통신회선설비 등을 이용하여 기간통신역무를 제공하거나,법령에서 정하는 바에 따라 구내에서 전기통신역무를 제공하는 사업자로서,국제전화서비스, 재판매 사업자 등이 해당.

즉, 자체망이 없이 직접설지채논 기간통신사업자의 통신설비를 임대하여 서비스를 제공하는 사업자이다.

기간통신사업자와 다르게 별도의 허가를 받지않고 정해진 절차에 따라 방송통신 위원회에 등록된 사업자

지역케이블, 알뜰폰통신사 등등

부가통신사업자

기간통신사업자의 정기통신회선 설비를 임차하여 기간 통신 역무 이외의 전기통신역무를 제공하는 사업자로서,

기본적인 통신서비스에 컴퓨터기능을 결합해서 통신서비스를 제공하는사업자로 흔히 우리가 일반적으로 쉽게 접하는 서비스 사업자 들이다.

포털사이트,게임사이트,온라인쇼핑몰,경매,커뮤니티,미니홈피,블로그 등 일반적인 인터넷 웹사이트 와 P2P 사이트 등을 운영하는 사업자가 해당된다.

부가통신사업자도 방송통신위원회에 정해진 절차에 따라 신고를 하면 사업자로 등록된다.

작성자: Eric Yoon / yoonsweety.eric@gmail.com

전기통신 사업자 2

영리목적의 정보제공 및 정보제공 매개자

영리를 목적으로 한다는 말은 재산상 이익을 취득하거나 이윤을 추구하려는 목적이 있다는 것을 의미.

학술,종교,자선단체등 비영리단체가 순수하게 해당 단체의 설립목적을 위해 웹사이트를 개설하여 운영하는경우는 정보통신서비스 제공자로 보기 어렵다.

하지만, 부수적인 목적으로 영리행위를 하는경우에는 정보통신서비스 제공자

준용사업자

통신사업자의 개인정보보호의무를 따르도록 되어 있는 사업자로서 여행업・호텔업, 항공운송사업, 학원・교습소, 휴양콘도미니엄업, 할인점・백화점・쇼핑센터, 체인사업을 영위하는 자

(-준용사업자는 개인정보보호법 을따라간다.!-)

(-준용사업자가 수탁업체일 경우 위탁업체의 유형을
따라간다[법 28 조기술적.관리적보호조치규정 준용)

<table>
<tr><td rowspan="6">망법
적용
대상자</td><td rowspan="4">방통위
고시
대상자</td><td rowspan="3">전기통신
사업자</td><td>기간통신사업자</td></tr>
<tr><td>별정통신사업자</td></tr>
<tr><td>부가통신사업자</td></tr>
<tr><td colspan="2">정보통신서비스 제공자로부터 개인정보를 제공받은 자</td></tr>
<tr><td colspan="2">개인정보의 수집/취급 및 관리 등을 위탁받은자</td></tr>
<tr><td colspan="2">영리를 목적으로 전기통신사업자의 전기통신역무를 이용
해 정보를 제공하거나 매개하는자</td></tr>
<tr><td>행안부
고시
대상자</td><td colspan="2">준용사업자</td></tr>
<tr><td colspan="3">다른 법률에서 망법의 개인정보보호 규정을 준수하도록 의무화한 자</td></tr>
</table>

작성자: Eric Yoon / yoonsweety.eric@gmail.com

OPT-IN

수신동의 = 선 동의

고객이 마케팅 메시지 수신에 동의하는 것. 판매자가 모바일 홍보 활동에서 이루어지는 양방향 상호작용에 관여하려면, 먼저 고객이 판매자의 쇼트 코드로 문자 메시지를 보내 동의 의사를 밝혀야 한다.

EU 방식 이다.

OPT-OUT

수신거부 = 선 서비스

광고성이나 음란성 메일 차단 방식의 하나로 수신자가 거부 의사를 밝혀야만 문자를 보낼 수 없도록 하는 방식

미국 자율 기업 방식.

CSR -기업의 사회적책임 Corposrate Social Responsibility

비즈니스모델에 통합된 기업의 자기규제적 형태를 의미

3P = people,Planet,Profit - (사회적책임,환경보호책임,경제적책임)

소비자의 개인정보를 보호함으로써 위험관리체계를 한단계 성숙시켜 기회창출과 브랜드를 차별화를 구현하고,규제의 간섭으로부터 자유로울수 있는권리 확보

지나친 강조가 기업자체의 이익목적이라는 비판과 개인정보의 활용으로 기업의 직접적 이익을 창출한다는 영향에 주의하자 !!!

작성자: Eric Yoon / yoonsweety.eric@gmail.com

해쉬 암호화

입력된 데이터를 자르고 치환하거나 위치를 바꾸는 등의 방법을 사용해 길이가 고정된 결과를 만든다.

보안강도	NIST(미국)	CRYPTREC(일본)	ECRYPT(유럽)	국내	안전성 유지기간 (년도)
80 비트 이상	SHA-1 SHA-224/256/384/512	SHA-1† SHA-256/384/512 RIPEMD-160	SHA-1 SHA-224/256/384/512 RIPEMD-160 Whirlpool	SHA-1 HAS-160 SHA-256/384/512	2010년까지
112 비트 이상	SHA-224/256/384/512	SHA-256/384/512	SHA-224/256/384/512 Whirlpool	SHA-256/384/512	2011년부터 2030년까지 (최대 20년)
128 비트 이상	SHA-256/384/512	SHA-256/384/512	SHA-256/384/512 Whirlpool	SHA-256/384/512	2030년 이후 (최대 30년)
192 비트 이상	SHA-384/512	SHA-384/512	SHA-384/512 Whirlpool	SHA-384/512	
256 비트 이상	SHA-512	SHA-512	SHA-512	SHA-512	

보안강도	NIST(미국)	CRYPTREC(일본)	ECRYPT(유럽)	국내	안전성 유지기간 (년도)
80 비트 이상	AES-128/192/256 2TDEA† 3TDEA†	AES-128/192/256 3TDEA Camellia-128/192/256 MISTY1	AES-128/192/256 2TDEA 3TDEA KASUMI Blowfish†	SEED ARIA-128/192/256	2010년까지
112 비트 이상	AES-128/192/256 3TDEA	AES-128/192/256 3TDEA Camellia-128/192/256 MISTY1	AES-128/192/256 Blowfish KASUMI 3TDEA	SEED ARIA-128/192/256	2011년부터 2030년까지 (최대 20년)
128 비트 이상	AES-128/192/256	AES-128/192/256 Camellia-128/192/256 MISTY1	AES-128/192/256 KASUMI Blowfish	SEED ARIA-128/192/256	2030년 이후 (최대 30년)
192 비트 이상	AES-192/256	AES-192/256 Camellia-192/256	AES-192/256 Blowfish	ARIA-192/256	
256 비트 이상	AES-256	AES-256 Camellia-256	AES-256 Blowfish	ARIA-256	

작성자: Eric Yoon / yoonsweety.eric@gmail.com

업무위탁

서비스제공을 위해 발생하는 업무의 일부를 다른 업체가 수행하는과정에서 개인정보 제공이 발생하는 것으로 자신의 업무와 직,간접적으로 관련된 업무로 ,제공하는 측의 사무처리를 위한 정보 제공.

개인정보보호 법에서는 위탁을 2 자의 업무로 보고 있다. 아웃소싱 !! 위탁 임을 잊지말자

위탁자

위탁에서 위임을하는자 가 위탁자 이며 수탁자를 직원관계로 보기 때문에 문제 발생소지를 막기 위하여 관리,감독을 한다.

수탁자

위탁자에게 위임을 받은자 이다.

3 자제공

위탁과는 전혀다르므로 확실히 구분을 하자.

3 자의 업무를 위한다.

즉 2 자의 업무를 전혀 하지도 않고, 제공 되는즉시 , 2 자의 책임도 없이 정보처리자는 3 자인 제공받는자가 책임을 진다.

계열사라 하더라도 업무부서가 다르면 제공이 될수 있다 .

작성자: Eric Yoon / yoonsweety.eric@gmail.com

손해배상

우리나라에서는 2가지 방식의 손해 배상제도가 있다. 피해 액수에 따라 각각의 장점을 파악해서 선택할수 있다.

1.징벌적손해배상

- 기업의 고의,또는 중과실로 정보주체에게 피해발생

재산,정신적피해 모구 포함 가능

대신 피해자 정보주체가 피해액을 입증 !! 당연하다 !

한도는 실제 피해액의 3배 까지 !!

2.법정 손해배상.

- 기업의 고의,또는 과실로 정보주체에게 피해 발생

법정으로 보상금액을 300만원 까지 책정 .....!!!!!

대신 피해자인 정보주체가 피해액 입증을 면제 할수 있음.

작성자: Eric Yoon / yoonsweety.eric@gmail.com

민감정보

사상.신념(사상적 경향,종교적신념)

노동조합,정당가입 (공식적이거나,적법한 노동조합이나 정당이 아니여도 된다) 비공식적인 조합도 포함.

정치적 견해

건강,성생활등에 관한정보 (병력,신체적,정신적장애,성적취향) = 신체적민감정보중 혈액형은 아니다 !!!!!

시행령의 민감정보

유전자정보,범죄경력에 관한정보.

시행령의 2 가지 민감정보는 공공기관에서 몇가지 업무를 수행할때 민감정보로 보지않는다 !!!!

보호위원회 심의,의결을 거친 경우

국제협정,조약 등 국제협정의 이행을 위해 필요한 경우

범죄수사를 위한 경우

법원의 재판업무

형및감호,보호처분의 집행을 위해필요한 경우

이때는 시행령의=대통령령 의 민감정보 2 가지 동의없이 처리가능하다!!!

유전정보,범죄정보 !!

작성자: Eric Yoon / yoonsweety.eric@gmail.com

IPS 침입방지

능동형 보안솔루션이라고도 불리는 IPS 는 인터넷 웜 등의 악성코드 및 해킹 등에 기인한 유해트래픽을 차단해 주는 솔루션이다.

IPS 는 공격탐지를 뛰어넘어 탐지된 공격에 대해 웹 연결을 끊는 등 적극적으로 막아주는 솔루션이라고 할 수 있다.

IPS 를 구분하자면

1.네트워크 기반 IPS 와 2.호스트 기반 IPS 로 크게 나눌 수 있다.

네트워크 기반 IPS 는 방화벽처럼 네트워크에 인라인 모드로 설치돼 공격을 차단해주는 기능을 하고 호스트 IPS 는 서버 애플리케이션을 담당하며 시큐어 OS 등과 비슷한 기능을 수행한다.

IPS 는 IDS 에서 한발 나아가 공격이 실제 피해를 주기 전에 미리 능동적으로 공격을 차단함으로써 공격 피해를 최소화할 수 있는 능동적 보안대책이라는 점이 가장 큰 장점이다. IPS 는 OS 나 애플리케이션의 취약점을 능동적으로 사전에 보완하고 웜이나 버퍼오버플로우, 특히 비정상적인(Ano-maly) 트래픽이나 알려지지 않은 공격까지 차단할 수 있기 때문에 한층 높은 보안을 제공해준다.

(새로운 공격 유형도 탐지 할수 있지만, 정상적인 서비스도 오경보로 탐지할수도 있는 담점이 있다.)

IDS 침입 탐지

특정 패턴을 기반으로 공격자의 침입을 탐지

(기존에 발표된 공격은 막지만 새로운 유형의 공격일 경우 허점이 있다)

작성자: Eric Yoon / yoonsweety.eric@gmail.com

비식별 관련 용어 정의

비식별

개인정보를 비식별 조치한정보 로써, 정보의 집합물에서 개인을 식별할수 있는 요소를 전부 또는 일부 삭제하거나 대체등의 방법을 통해 개인을 알아볼수 없도록 하는 조치

1.가명처리

홍길동,35 세,서울거주,한국대 재학 > 임ㄲ ㄱ정,30 대,서울거주,국제대 재학

2.총계처리

임꺽정 180cm,홍길동 170cm,콩쥐 160cm,팥쥐 150cm>물리학과 학생 키 합 660cm, 평균키 165cm

3.데이터삭제

주민등록번호 901227-1234567 > 90 년대 남자

4.데이터범주화

홍길동,35 세>홍씨,30~40 세

5.데이터마스킹

홍길동,35 세,서울거주,한국대재학,010-1234-5678 >홍*동,35 세,서울거주,**대재학,010-****-5678,생년월일****년**월**일

(정보집합물에 포함된 식별자,속성자 는원칙적으로 삭제조치하여야한다.

단, 데이터 이용목적상 반드시 필요한 식별자는 가명처리,총계처리 등 비식별조치후 활용가능

식별자

개인또는 개인과 관련한 사물에 고유하게 부여된 값

예) 고유식별번호,성명,주소,전화번호,통장계좌번호,사진 등등

작성자: Eric Yoon / yoonsweety.eric@gmail.com

속성자

개인과 관련된 정보로 다른정보와 쉽게 결합하는 경우 특정 개인을 알아볼수 있는정보

개인특성(나이,고향,동호회,취미,종교,흡연여부...등등)

신체특성(혈액형,진료내역,투약코드,병명,장애유형...등등)

신용특성(세금납부액,신용등급,의료급여자 등등)

경력특성(학교명,학과명,성적,학력,경력,직업,직종,부서명,직장명..등)

전자적특성(쿠키정보,접속일시,방문일시,서비스이용기록,접속로그,휴대전화사용기록 등등)

가족특성(배우자, 자녀,부모, 가족정보,법정대리인정보 등등)

특히 희귀병명,희귀경력 등의 속성자는 구체적인상황에서 개인식별 가능성이 매우 높으므로 엄격한 비식별조치가 필요하다.

거버넌스

여러업무를 관리하기위해 정치,경제및 행정적권환을 행사하는방식으로써,
일종의 국정관리 체계라고 의미를 생각하자.
현재,우리는 정보보안을 말하고 있으므로 IT, Security 법,명령등을 준수 한다라고 해석하면될것같다
리더쉽,조직구조,프로세서통제,관리체계 구성
정보보호에대한전략과 통제체계를규정하는 보안정책

컴플라이언스

거버넌스가 법률,정책,체계를 의미 하면 컴플라이언스는
이에따른 준수를 의미함.
해당되는법규제요건을 만족하고,정보보호관리 프라임워크구축,운영
노력을 의미함.

작성자: Eric Yoon / yoonsweety.eric@gmail.com

GDPR 에 사용되는 기본적인 용어.

국내법의 용어와 비슷한 부분도 있지만, 범위와 역할의 차이가 상이하니 꼭 확인해보도록 하자

GDPR

유럽연합의 개인정보보호법이다. 2018 년 5 월 25 일 시행이됨. 정보주체의 권리와처리자의 의무를 대폭강화 하며, 위반시 막대한 과징금을 부과 함으로 우리 기업의 적절한 컴플라이언스를 통해 유럽연합 시장에 원활히 진출 하도록 유의해야할 것이다.

ONE-STOP-SHOP 매커니즘

처리되는 개인정보의 정보주체가 EU 내 여러국가에 흩어져있는 경우 주사업장이나 단일 사업장이 소속된 국가의 감독기구가 선임 감독기구의 역할을 수행하면서 다른 회원국의 감독기구와 수시로 협력 함으로써 컨트롤러 프로세서는 하나의 감독 기구만을 대상으로 대응 가능한 매커니즘

DPO (Data protecition Officer)

조직이 개인정보보호 관련 법률을 준수하고 개인정보보호 의무를 다하도록 조언 및 도움을 주는 역할로써 내부직원 또는 외부 인사로 지정할수 있다.

(우리나라의 책임자 역할로 비슷하지만,지정요건,책무,자격,등이 상이함으로 우리말로 번역했을 경우 혼동을 방지하고자 영어원문 그대로 사용)

컨트롤러 (Controller)

개인정보 처리의 목적과 수단을 결정하는 주체를 의미

자연인을 포함한 법인,정부부처,기타 단체등

(우리나라 처리자와 비슷한 의미)

프로세서 (Processor)

컨트롤러를 대신하여 개인정보를 처리하는 자연인,법인,정부부처관련기관,간체등

(수탁자 로생각하자)

작성자: Eric Yoon / yoonsweety.eric@gmail.com

제 3 자 (Third party)

직접적권한으로 개인정보를 처리할수 없는 개인제외 한
모든자연인,법인,정부부처,관련기관,단체 등등

(우리나라 3 자와 비슷)

수령인 (Recipient)

제 3 자 여부와 관계없이 개인정보를 공개,제공받는 자연인,법인,정부부처,단체 등등

단, 특정한문의,회신, 조회 업무를 수행하기위해 개인정보를 제공받는 정부부처는 수령인에 해당되지 않는다. -세관, 금융시장 당국

(수령인은 우리나라의 정보주체 로 생각하면 쉽다.)

프로파일링 (Profiling)

개인의 특징을 분석하거나 예측하는등 해당 개인의 특성을 평가하기 위하여 행해지는
모든형태의 자동화된 개인정보처리 이다

정보사회서비스 (Information Society Service)

서비스를 제공받는자의 개별적 요청에 따라 원격에서 전자적 수단을 통하여 통상
영리목적으로 제공되는 서비스를 의미

원격 (at a distance)

서비스 제공자와 해당서비스를 제공받는자가 동시에 물리적으로 같은 장소에 있을 것을 요구하지 않는다.

전자적 수단을 통하여 (by electronic means)

전자적 장비로 데이터를 처리하여 서비스가 제공되는 것을 의미

서비스를 제공받는자의 개별적 요청에 따라 (at the individual request of a recipient of services)

개별적 요청을 바탕으로 한 데이터 전송에 의해 서비스가 제공되는 것을 의미.

작성자: Eric Yoon / yoonsweety.eric@gmail.com

국내법과 비교표

[참고-Kisa 우리기업을위한개인정보보호법]

한국(개인정보보호법)	EU(GDPR)	비고
민감정보(특별한 유형의 개인정보)		
[제23조제1항] 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(유전자 검사 등의 결과로 얻어진 유전정보 및 '형의 실효 등에 관한 법률' 제2조제5호에 따른 범죄경력 자료에 해당하는 정보)(이하 '민감정보'라 한다)를 처리해서는 아니된다.	[제9조] 컨트롤러는 인종·민족, 정치적 견해, 종교적·철학적 신념, 노동조합의 가입 여부를 나타내는 개인정보의 처리와 유전자 정보, 개인을 고유하게 식별할 수 있는 생체 정보, 건강 정보, 성생활·성적 취향에 관한 정보를 처리해서는 안 된다. [제10조] 범죄경력 및 범죄행위에 관련된 개인정보의 처리 또는 제6조제1항에 근거한 관련 보안조치는 공적권한의 통제 하에서 또는 그 처리가 정보주체의 권리 및 자유를 위한 적절한 안전장치를 규정하는 EU 또는 회원국 법이 허가하는 경우에만 수행되어야 한다.	GDPR은 특별한 유형의 개인정보(민감정보)와 범죄경력 및 범죄행위에 관련한 개인정보를 구분하고, 그 처리 기준을 구분하였음
위탁자	컨트롤러	
[제26조제2항] 위탁자는 개인정보의 처리 업무를 위탁하는 개인정보처리자를 의미한다. 위탁자는 자신의 사무 처리를 위해 통상 직접 수집한 개인정보를 수탁자에게 제공한다.	[제7조] 컨트롤러는 개인정보 처리의 목적과 수단을 결정하는 주체를 의미한다. 컨트롤러는 개인정보 처리의 목적과 수단을 규정하기만 하면 족하며, 자신이 개인정보를 직접 수집하여 프로세서에게 제공할 필요는 없다.	GDPR의 컨트롤러는 처리의 목적과 수단을 규정하는 역할을 하며, 반드시 정보의 처리를 위탁할 필요는 없음
수탁자	프로세서	
[제26조제2항] 수탁자는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자를 의미한다.	[제8조] 프로세서는 컨트롤러를 대신하여 개인정보를 처리하는 개인, 법인, 정부부처 및 관련기관, 기타 단체 등을 의미하며, 컨트롤러의 지시에 따라 개인정보를 처리한다.	
개인정보 보호책임자	DPO	
[제31조제1항] 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다. [시행령 제32조제2항] 개인정보처리자는 법 제31조제2항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정한다. 1. 공공기관 : 다음 각 목의 구분에 따른 기준에 해당하는 공무원 등 2. 공공기관 외의 개인정보처리자 : 다음 각 목의 어느 하나에 해당하는 사람 가. 기업주 또는 대표자 나. 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)	[제37조제5항] DPO는 전문적 자질, 특히 개인정보보호법과 실무에 대한 전문적 지식 및 제39조에 언급된 직무를 완수할 능력에 근거하여 지정되어야 한다. [제39조제1항] DPO는 최소한 다음의 직무를 가져야 한다. (a) 컨트롤러나 프로세서, 그리고 데이터 처리를 수행하는 해당 직원에게 GDPR과 EU 또는 회원국의 개인정보보호 조문에 따른 의무에 대하여 고지하고 조언 (b) GDPR과 EU 또는 회원국의 개인정보보호 조문에 대한 컨트롤러 또는 프로세서의 정책 준수 여부를 모니터링(직원 교육과 감시 활동 포함) (c) 요청이 있을 경우, 개인정보보호 영향평가에 관한 자문을 제공하고 평가 이행 상황을 감시 (d) 감독기구와의 협력 (e) 사전협의 등 처리에 관련된 사항에 대한 감독기구의 연락처 역할을 수행하며, 적절한 경우에는 기타 사안에 대한 자문을 제공	국내법 상 개인정보보호책임자의 자격요건은 공무원 또는 사업주, 대표자, 임원 등 일정 지위로 구분하나, GDPR 상 DPO는 전문적 자질, 특히 개인정보보호법과 실무에 대한 전문적 지식 및 제39조에 언급된 직무를 완수할 능력에 근거하여 지정되어야 함

작성자: Eric Yoon / yoonsweety.eric@gmail.com

-
-
- 무료, 공개 스터디 카페 입니다.
- 배포 자유!! 하지만 수정은 금지 합니다. !! (힘들게 제작한 제작자 입니다)
- 비영리 목적으로 순수 하게 학습이 목표 입니다.
- 순수한 학습 목적 이기에 검색 엔진에서 검색이 되던 안되던, 신경 쓰고 있지 않습니다.
- 그렇기 때문에, 학습 하며 작성한 자료를 이미지 그대로 첨부 하였습니다.
- 순수한 학습 목적 이기에 검색 엔진에서 검색이 되던 안되던, 신경 쓰고 있지 않습니다.
- 잘못된 부분이나, 수정될 부분이 있으면 피드백 주시는되로 즉시 수정 하도록 노력하겠습니다.
- KISA, google, Naver 사의 위키피디아,이미지 를 사용 하였습니다. 문제시, 즉시 삭제 하도록 하겠습니다.

[참고 자료]
개인정보보호법령
정통망법령
표준개인정보보호지침- 행정안전부 고시
개인정보의 안전성확보조치 기준 -행정안전부 고시
정보통신망 이용촉진 및 정보보호 등에 관한법률 기술적,관리적 보호조치기준
방송통신위원회 고시
Kisa-우리기업을위한개인정보보호법 지침자료
비식별가이드

작성자: Eric Yoon / yoonsweety.eric@gmail.com