

개인정보보호법 상담사례집

2012. 2



행정안전부

KISA 한국인터넷진흥원
Korea Internet & Security Agency



개인정보보호법 상담사례집

2012. 2



행정안전부

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목차

제1장 개인정보보호법 일반

- Q1 개인정보보호법에서 보호하는 개인정보는 구체적으로 어떤 정보 인가요? / 13
- Q2 이메일과 다크네임만 수집해도 개인정보로 볼 수 있나요? / 14
- Q3 시군구에 자동차과태료 검색 웹페이지에서 “이름 + 주민등록번호 앞자리 + 차량번호” 3가지를 맞게 입력하면 해당 차량에 대한 과태료가 검색됩니다. 개인정보에 해당될까요? / 14
- Q4 개인정보보호법 시행으로 개인정보 보호의무를 지는 대상, 즉 적용 대상 및 범위가 달라지나요? / 14
- Q5 개인정보보호법에서는 개인정보파일의 범위가 확대된다는 말이 있던데 기존과 다른가요? / 15
- Q6 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 신용정보의 이용 및 보호에 관한 법률 중에 어느 법이 더 우선적용 되나요? / 15
- Q7 영리법인이 아닌, 후원, 기부 재단의 경우에도 개인정보보호법 적용 대상인가요? / 16
- Q8 개인정보보호법에서 말하는 공공기관의 범위는 어디까지 인가요? / 16
- Q9 개인정보보호법 적용에서 일부 제외되는 경우는 어떤 경우인가요? / 18
- Q10 동창회, 동호회 등 친목도모 단체의 적용이 일부 제외되는 조항은 몇 조 인가요? / 19



제2장 개인정보의 수집, 이용, 제공

- Q1** 홈페이지 구인게시판에 게시물 작성자가 본인의 필요에 의해서 휴대전화 번호를 기재하는 경우 개인정보를 수집하게 되는 것인가요? / 20
- Q2** 졸업앨범에 있는 개인정보를 수집하여 전화 TM 등에 활용해도 되나요? / 20
- Q3** 기업정보를 수집하여 활용하는 것도 개인정보보호법상 동의를 받아야 하나요? / 20
- Q4** 쇼핑몰에서 비회원 주문이나 게시판의 경우도 개인정보 수집동의를 받아야 한다고 하던데요. 이름과 이메일 2가지 정도만 수집하더라도 동의를 받아야 하나요? / 21
- Q5** 신규로 직원들을 뽑을 때 이력서에 개인정보 수집 동의를 받아야 하나요? / 21
- Q6** 만14세 미만 아동의 법정대리인을 포함한 정보주체의 동의를 받는 방법에는 어떤 것이 있나요? / 22
- Q7** 병원에 방문한 만14세 미만 아동에게도 법정대리인의 동의를 받아야 하나요? / 22
- Q8** 병원에 내원한 환자들에 대해서도 개인정보 수집 동의서를 받아야 하나요? / 23
- Q9** 동호회의 경우 이름과 연락처 정도 수집이 되는데 이때 모두 동의 받아야하고, 이 데이터를 컴퓨터에 저장시 암호조치를 해야 하나요? / 23
- Q10** 종교단체가 선교목적으로 개인정보를 동의 없이 수집할 수 있나요? / 24

목차

- Q11** 관공서에서 행사가 있을때 초청장을 보낼 때도 동의서를 받아야 하나요? / 24
- Q12** 공공기관에서 개인정보를 포함하여 게시하는 경우가 있는데 이럴 경우에도 어떤 조치를 해야 하나요? / 24
- Q13** 벌과금 등 관련한 공시송달 공고를 검찰청 홈페이지 “고시/공고”란에 “성명, 징제번호, 등기번호, 수령여부” 네 가지 항목을 포함하여 게시할 경우, 개인정보보호법에 저촉되나요? / 25
- Q14** 개인정보보호법 제15조 제2항 제4호의 내용에 “동의를 거부할 권리가 있다는 사실 및 동의의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용”을 기재하여야 한다고 했는데 불이익의 내용에 신청 또는 이용 불가라고 기재하여도 위법은 아닌가요? / 25
- Q15** 개인정보보호법 제15조 제3항에 보면 “공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우”라고 되어있습니다. 여기서, 법령 등의 범위와 불가피한 경우란 무엇인가요? / 26
- Q16** 공공기관인데 감사부서나 상급기관에서 감사 목적으로 개인정보의 제공을 요청하는데 동의 없이 제공할 수 있나요? / 27
- Q17** 수기로 작성된 신청서를 바탕으로 전산시스템에 등록하여 실적 등을 관리하게 되는데, 신청서에 등록에 대한 안내를 넣으면 신청서에 있는 개인정보를 전산시스템에 등록 및 활용하는 것이 가능 한가요? / 27
- Q18** 종이계약서를 작성하는 사업자의 경우 계약의 이행을 위해서 주민등록번호를 수집할 경우에도 정보주체의 별도 동의가 필요하나요? / 28
- Q19** 학교에서는 행사에 참여하는 학생의 사진, 학교명과 이름을 팸플릿에 넣거나 학교 홈페이지에 학생들의 생활 사진이나 행사와 관련된 사진 등을 게시하게 되는데, 개별적으로 학생들의 동의를 받아야 하나요? / 28



- Q20** 개인 블로그 등에서도 개인정보 수집이 이루어지는데 이 경우에도 동의절차 및 보호조치를 만들어야 하나요? / 29
- Q21** 오픈 마켓에서 물건을 판매하는 업체인데, 수집할 때 별도의 동의 없이 휴대전화번호만 받는 것도 문제가 되나요? / 29
- Q22** 교육접수가 중복되는 것을 방지하기 위해 접수시에는 생년월일과 성별까지만 수집을 하고, 실제 교육을 신청할 때에는 이름만 받고자 할 경우 동의가 없어도 되나요? / 29
- Q23** 개인정보를 제3자에게 제공할 수 있는 방법이 있나요? / 30
- Q24** 자체 수집한 정보가 아니고 다른 기관에서 입수한(제공받은) 자료도 활용이 가능한가요? / 31
- Q25** 개인정보 처리업무 위탁에 대한 원칙 및 방법은 무엇인가요? / 31
- Q26** 내부 직원에 대한 교육을 외부 업체에 위탁할 때 위탁에 대한 동의를 받아야 하나요? / 32
- Q27** 재개발을 하기 위하여 주민자치회에서 주민들의 의견을 수렴하기 위해 기존에 수집한 개인정보(이름, 주민등록번호, 주소, 전화번호)를 이용하여 우편물을 발송해도 되나요? / 32
- Q28** 퇴사한 직원에 대한 근무기록 등은 퇴사 후 몇 년간 보관하면 되나요? / 33
- Q29** 채용을 위해서 개인정보를 수집하고 퇴직하고 나서 개인정보를 20년 동안 보유한다는 것에 동의를 받으면 문제가 없나요? / 33
- Q30** 개인정보 수집동의서를 받아서 처리할 경우 동의서 내용에 보유 및 이용기간은 개인정보처리자의 필요에 의해 보유기간을 정하면 되는 건가요? / 34
- Q31** 서비스 계약과 관련하여 개인정보 보유기간 설정을 어떻게 해야 하나요? / 35

목차

Q32 개인정보의 파기 시기 및 방법은 어떻게 해야 되나요? / 35

Q33 개인정보 파기시 예외 경우가 있나요? / 35

Q34 쇼핑몰에서 탈퇴한 회원들의 개인정보를 파기하려고 하는데, 일부 회원들은 할부 요금이 아직 미납되었거나 제품 A/S 기간이 남아 있습니다. 이러한 경우에는 어떻게 해야 하나요? / 36

Q35 개인정보를 정정·삭제 요청할 수 없는 경우도 있나요? / 36

제3장 개인정보의 처리

가. 민감정보의 처리제한

Q1 개인정보정보(or 개인건강정보) 중 “개인을 알아볼 수 있는 정보”가 개인정보 인가요? 아니면 개인정보정보(or 개인건강정보) 전체가 개인정보 인가요? / 37

Q2 환자로부터 수집하지 않고 각 의료기관에서 자체 발급하는 병록번호는 개인정보 인가요? 그리고 병록번호에 연결된 건강정보는 개인정보 인가요? / 37

Q3 개인정보보호법 제15조(개인정보의 수집·이용)에서 의료기관의 개인정보정보(개인건강정보) 수집은 동의 대상인가요? / 38

Q4 개인정보보호법 제23조(민감정보의 처리 제한)에서 건강, 성생활을 민감정보로 정의하고 처리하지 말 것을 규정하고 있는데 병원에서 건강정보를 수집할 수 있나요? / 38

Q5 신규 환자가 아닌 기존 환자에 대한 동의는 어떻게 받아야 하나요? / 39



나. 고유식별정보의 처리제한

- Q1** 홈페이지를 통하여 주민등록번호를 수집하는 경우 정보주체에게 별도 동의를 받으라고 하는데 별도 동의 받는 적절한 방법에는 무엇이 있나요? / 39
- Q2** 기존주민등록번호를 “111111-1xxxxxx”로 변환하여 보유하려 하는데 이러한 데이터가 개인정보보호법에서 규정하고 있는 고유식별정보에 해당이 되나요? / 40
- Q3** 기존에 가지고 있던 주민등록번호는 폐기해야 하나요? 아니면, 전체 회원에 대해 다시 동의 절차를 받아야 하나요? / 40
- Q4** 사원증 번호, 회원번호 등 개인에게 고유하게 부여되는 번호도 고유식별정보의 범위에 포함되나요? / 41
- Q5** 여권판독기로 여권정보를 확인하여 고객의 호텔 예약을 확인하고 있는데 개인정보보호법에 위반이 되나요? / 41
- Q6** 주민등록번호 대체수단 의무도입은 어떤 경우에 해야 하나요? / 41
- Q7** 건물 출입시에 신분확인하고 출입증 교부를 위해서 성명을 적고 신분증을 받아 보관하는 경우 개인정보 및 고유식별정보 수집·이용 동의서를 받아야 하나요? / 41
- Q8** 병원의 경우 주민등록번호 수집·이용이 필수인데 주민등록번호 대체 수단 마련이 의무화되나요? / 42
- Q9** 읍면동에서 민원인이 공공 아이핀을 신청하는 업무가 있습니다. 만일 만14세 미만 아동이 공공 아이핀을 신청하는 경우 법정 대리인과 동행하여 신청해야 하나요? / 42

목차

다. 영상정보처리기기의 설치·운영 제한

- Q1 사람을 촬영하지 않아 개인정보 침해 위험이 전혀 없는(안개, 황사 등의 기상상황 파악) 영상정보처리기기에 대하여 개인정보보호법이 적용 되나요? / 43
- Q2 영상정보처리기기(CCTV)는 언제 설치할 수 있나요? / 43
- Q3 CCTV를 목욕탕 휴게실, 수면실 등에 설치할 수 있나요? / 44
- Q4 직장에서 작업감시를 위해 CCTV를 설치하려면 어떤 기준에 따라야 하는지요? / 45
- Q5 CCTV를 따로 녹화하지는 않고 관찰만 하고 있는데 이런 경우에도 개인정보보호법에 해당이 되나요? / 45
- Q6 버스회사에서 폭행사건, 범죄예방 등을 파악하기 위해 CCTV 녹음 기능을 사용하고 싶은데 가능한가요? / 45
- Q7 개인정보보호법 제25조에 따라 공개된 장소에 설치되는 영상정보 처리기기에 대하여 적용이 일부 제외되는 조항은 어떤 것이 있나요? / 46
- Q8 건물 밖에 여러 대의 CCTV가 설치되어 있는 경우 안내판을 각각 설치해야 하나요? / 46
- Q9 개인정보보호법상 운영 중인 영상정보처리기기에 목적을 추가할 경우 어떤 절차를 거쳐야 하나요? / 46
- Q10 영상정보처리기기를 다목적용(시설안전, 주차관리, 범죄예방 등)으로 이용하고 통합관리 하는 경우 안내판에 “다목적용”이라고 표기하면 되나요? / 47



라. 업무위탁에 따른 개인정보의 처리제한

- Q1 사업자가 고객의 DM발송을 타 업체에 위탁할 경우 동의가 필요한가요? / 47
- Q2 포인트 카드사와 제휴를 맺어 결제시 포인트로 결제할 수 있도록 하려면 어떻게 해야 하나요? / 47
- Q3 외국계 회사로 내부인사시스템의 관리는 외국의 본사에서 관리하고, 직원들의 개인정보는 한국지사를 거쳐 외국의 본사로 전달이 되며, 외국본사는 다시 외국의 타 회사에 관리업무를 위탁하여 처리를 하고 있습니다. 이 경우 직원들의 동의를 받아야 하나요? / 48
- Q4 고객만족도 조사를 위해 이름과 전화번호를 위탁업체에 제공하게 되는데 이 경우 동의를 받아야 하나요? / 48

제4장 개인정보의 안전한 관리

가. 안전조치 의무

- Q1 개인정보의 안전성 확보조치는 무엇인가요? / 49
- Q2 소기업 및 소상공인 지원을 위한 특별조치법에 따른 소상공인입니다. 내부관리계획을 수립하지 않아도 되나요? / 49
- Q3 내부 직원의 인사정보와 외부 전문가 정보 등의 DB를 관리하고 있습니다. 개인정보보호법에 따라서 별도의 안전장치를 해야 하나요? / 50
- Q4 이전에 수집한 개인정보도 모두 암호화해야 하나요? / 50
- Q5 주민등록번호를 저장하면 무조건 암호화해야 하나요? / 51

목차

- Q6 국내에 있는 직원의 DB가 해외 시스템에 있는데 암호화를 해야 하나요? / 51
- Q7 비디오 대여점에서 고객관리를 위해 업무용 컴퓨터를 운영하고 있는데, “개인정보의 안전성 확보조치 기준”에 따라 어떠한 조치가 필요 한가요? / 52
- Q8 백화점에서 고객정보 데이터베이스를 운영하고 있습니다. 개인정보 암호화 대상이 무엇이며 어떻게 해야 하나요? / 52
- Q9 전산실 또는 자료보관실이 없는 중소기업입니다. “개인정보의 안전성 확보조치 기준” 제10조(물리적 접근방지) 조항을 준수해야 하나요? / 53
- Q10 개인정보보호법 시행 이후 개인정보 안전성 확보조치(암호화 등), 주민등록번호 대체수단, 영향평가 등은 유예기간이 언제까지 인가요? / 53
- Q11 개인정보를 암호화해야 하는데 어떤 정보를 어디까지 암호화해야 하나요? / 53
- Q12 개인정보 DB가 내부에 관리되면 암호화조치를 반드시 해야 하나요? / 54
- Q13 고유식별정보인 여권번호(9자리)중 일부(3~4자리)를 유일한 키를 생성하기 위해 사용할 경우에도 DB암호화가 필수사항인지요? / 54
- Q14 비밀번호에 대해 필수로 8자리를 하는 것이 맞나요? / 55
- Q15 내부관리계획을 세워야 한다고 나와 있는데 내부관리계획과 지침을 같은 것으로 보는지, 지침이 있다면 계획은 수립하지 않아도 되나요? / 55



나. 개인정보 처리방침의 수립 및 공개

- Q1 각각의 사이트들마다 각각 “개인정보 처리방침”을 고지해야 하나요? / 56
- Q2 오프라인에서 회원가입 후 온라인상에서 주민등록번호와 이름을 입력하여 회원 가입 유·무를 확인하는데 개인정보 취급 또는 처리 방침을 세워야 하나요? / 56
- Q3 개인정보보호법상 ‘개인정보 처리방침’, 정보통신망 이용 촉진 및 정보보호 등에 관한 법률상 ‘개인정보 취급방침’ 중 어느 것을 사용해야 하나요? / 57
- Q4 사업자인데요, 개인정보보호법 시행으로 개인정보취급방침을 어떻게 바꿔야 하나요? / 57

다. 개인정보 보호책임자의 지정

- Q1 자원봉사자의 정보를 저장하는 통합관리 사이트를 운영하는 경우에도 개인정보 보호책임자를 반드시 두어야 하고 파일도 출력물로 관리해야 하나요? / 58
- Q2 소규모 개인사업자도 개인정보 보호책임자를 지정해야 하나요? / 58

라. 개인정보파일의 등록 및 공개

- Q1 개인정보파일의 등록 및 공개는 무엇인가요? / 58
- Q2 직원들의 PC내 보유중인 업무관련자 연락처도 행정안전부장관에게 등록 및 공개해야하는 대상이 되는지요? / 59

목차

마. 개인정보 영향평가

Q1 공공기관은 영향평가를 무조건 해야 하나요? / 59

Q2 2011년 3월부터 IT시스템 재구축을 시작하여 2012년 12월 31일까지 진행되는 프로젝트로 해당 프로젝트는 설계까지 마무리 되었고, 현재 개발을 진행 중에 있습니다. 이 경우 기존 시스템으로 인정되어 5년 내에 영향평가를 받아도 되나요? / 60

바. 개인정보 유출통지

Q1 개인정보 유출 통지는 어떤 방법으로 하나요? / 60

Q2 홈페이지 자체 점검시 게시자의 부주의로 인하여 개인정보가 홈페이지에 게재되어 있는 것을 알게 되었다면 유출사고가 아니더라도 정보주체에게 통지해야 하나요? / 61

제5장 개인정보단체소송

Q1 단체소송은 무엇인가요? / 62

Q2 개인도 단체소송을 제기할 수 있나요? / 62

Q3 단체소송의 대상과 청구범위는 어떻게 되나요? / 63

Q4 단체소송에서 전속관할이 무엇인가요? / 63



제1장

개인정보보호법 일반

Q1

개인정보보호법에서 보호하는 개인정보는 구체적으로 어떤 정보인가요?

개인정보는 일반적으로 “특정 개인을 식별하거나 식별할 수 있는 정보”를 의미합니다. 즉, 개인과 관련된 일체의 정보는 모두 개인정보에 해당할 수 있습니다(예 : 성명, 주소, 연락처, 직업 등). 또한 개인정보에는 해당 개인과 직접 관련이 있는 정보뿐만 아니라, 그 개인에 대한 타인의 의견, 평가, 견해 등 제3자에 의해 생성된 간접적인 정보(예 : 신용평가 정보)도 해당될 수 있습니다.

개인정보보호법 상의 개인정보 정의는 다음과 같습니다.

1. 개인에 관한 정보

법률상의 개인정보는 “자연인(自然人)에 관한 정보”만 해당됩니다. 법인(法人)이나 단체의 정보는 법률에 따라 보호되는 개인정보의 범위에는 해당되지 않습니다.

2. 생존하는 개인에 관한 정보

법률상의 개인정보는 “생존하는 자연인”에 관한 정보만 해당됩니다. 따라서 이미 사망하였거나 민법에 의한 실종선고 등 관계 법령에 의해 사망한 것으로 간주되는 자에 관한 정보는 법률상의 개인정보로 볼 수 없습니다.

3. 생존하는 특정 개인을 알아볼 수 있는 정보

법률상의 개인정보에 해당되기 위해서는 그 정보로 “특정 개인을 알아볼(식별할)” 수 있어야 하며, 해당 정보만으로는 특정 개인을 식별할 수 없다 하더라도 “다른 정보와 쉽게 결합” 하여 식별 가능하다면, 개인정보에 해당됩니다. 예를 들어, 단순히 “성명” 정보만 있다면 특정 개인을 식별하는 것이 쉽지 않으나(동명이인 등), 개개인의 “주소 · 연락처” 등과 결합되어 특정한 개인을 식별할 수 있다면 개인정보로 볼 수 있습니다.



Q2

이메일과 닉네임만 수집해도 개인정보로 볼 수 있나요?

개인정보보호법 제2조제1호에 의거하여, 이메일주소는 다른 정보와 쉽게 결합하여 개인을 식별할 수 있는 정보에 해당한다고 보이기 때문에, 이메일과 닉네임만 수집하는 경우에도 개인정보보호법의 적용을 받는 것으로 해석될 수 있습니다.

※ 개인정보보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다

1. “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.

Q3

시군구에 자동차과태료 검색 웹페이지에서 “이름 + 주민등록번호앞자리 + 차량번호” 3가지를 맞게 입력하면 해당 차량에 대한 과태료가 검색됩니다. 개인정보에 해당될까요?

개인정보는 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보뿐만 아니라, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것은 모두 개인정보에 포함됩니다.

따라서 성명, 생년월일(주민등록번호 앞자리), 차량번호가 조합될 경우에는 개인정보에 해당합니다.

Q4

개인정보보호법 시행으로 개인정보보호 의무를 지는 대상, 즉 적용대상 및 범위가 달라지나요?

개인정보보호법 시행 이전에는 개별법이 있는 경우에 한해 개인정보보호 의무가 있었습니다



※ 공공기관(공공기관의 개인정보보호에관한법률), 정보통신서비스제공자 및 준용사업자(정보통신망 이용촉진 및 정보보호 등에 관한 법률), 신용정보 제공·이용자(신용정보의 이용 및 보호에 관한 법률).

개인정보보호법 시행 이후, 공공·민간부문의 모든 개인정보처리자가 적용대상이 됩니다. 즉, 제조업, 서비스업 등 72개 업종 320만 전체 사업자 대상이며, 중앙행정기관은 물론 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관과 협회·동창회 등 비영리단체도 대상이 됩니다.

Q5

개인정보보호법에서는 개인정보파일의 범위가 확대된다는 말이 있던데 기존과 다른가요?

정보통신망 이용촉진 및 정보보호 등에 관한 법률은 정보통신서비스제공자 및 준용사업자에 국한되었지만, 개인정보보호법은 전 영역에 걸쳐서 적용되는 법률입니다. 또한, 온·오프라인 구분 없이 개인정보보호법이 적용됩니다.

개인정보보호법 제2조 제4호는 “개인정보파일이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.”라고 규정하고 있습니다. 이는 개인의 이름이나 고유식별인자 등을 사용하여 색인·분류되어 있는 등 일정한 기준에 따라 쉽게 개인정보를 검색할 수 있도록 체계적으로 배열 또는 구성된 개인정보의 집합물을 말하는 것으로, 전자적 형태와 수기파일이 모두 해당됩니다. 수기문서로 작성된 병원의 진료카드파일, 회원모집 서류파일, 행정민원 서류파일 등도 개인정보파일에 해당됩니다.

Q6

개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 신용정보의 이용 및 보호에 관한 법률 중에 어느 법이 더 우선적용 되나요?

개인정보보호법 제6조에 따라 개인정보보호에 관해서는 다른 법률에 특별한 규정이 있는 경우에는 다른 법률을 우선 적용하고, 다른 법률이 없는 경우에만 이 법을 적용하도록 하고 있습니다. 즉, 다른 법률에서 특별히 개인정보보호법의 기준보다 강화하거나



완화하는 내용의 조문이 있는 때에만, 해당 조문별로 개인정보보호법의 적용을 배제합니다. 하지만 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 및 신용정보의 이용 및 보호에 관한 법률등이 적용된다고 하여, 해당 법률의 적용을 받는 자에 대하여 개인정보보호법 법 전체의 적용을 전면적으로 배제하는 것은 아닙니다.

정보통신망 이용 촉진 및 정보보호 등에 관한 법률 등에 규정되어 있지 않은 주민등록번호 등 고유식별정보 처리제한, 영상정보처리기기 설치운영 제한, 개인정보 유출 통지, 집단분쟁조정, 권리침해 중지 단체소송 등은 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 상의 정보통신서비스제공자에게도 모두 적용됩니다.

Q7

영리법인이 아닌, 후원, 기부 재단의 경우에도 개인정보보호법 적용 대상인가요?

개인정보보호법은 개인정보보호에 관한 일반법이므로, 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인(이를 동법 제5조에서 “개인정보처리자”라고 정의합니다)에 모두 적용됩니다. 따라서 비영리법인인 기부재단에도 개인정보보호법이 적용됩니다.

Q8

개인정보보호법에서 말하는 공공기관의 범위는 어디까지 인가요?

공공기관은 개인정보보호법 제2조제6호에 규정되어 있습니다.

1. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관

- ① 국회의 행정사무를 처리하는 기관 : 국회 사무처
- ② 법원의 행정사무를 처리하는 기관 : 법원 행정처
- ③ 헌법재판소의 행정사무를 처리하는 기관 : 헌법재판소 사무처
- ④ 중앙선거관리위원회의 행정사무를 처리하는 기관 : 중앙선거관리위원회 사무처

2. 중앙행정기관 및 그 소속기관

- ① 중앙행정기관(대통령 소속 기관 및 국무총리 소속 기관 포함)
 - 중앙행정기관은 전국적인 규모로 대국민 행정을 하는 기관으로서 「정부조직법」



제2조제2항에 따른 중앙행정기관(부·처·청)을 말함

- 또한 「정부조직법」 제5조의 합의제 행정기관 중에서 “중앙행정기관”에 해당하는 방송통신위원회, 공정거래위원회, 금융위원회, 국민권익위원회, 국가인권위원회, 진실·화해를 위한 과거사정리위원회가 해당됨¹⁾

② 중앙행정기관의 소속 기관

- 중앙행정기관이 그 소관 사무의 수행을 위하여 설치·운영하는 「정부조직법」 제3조의 특별지방행정기관(지방체신청, 지방국세청 등), 제4조의 부속기관(시험연구기관, 교육훈련기관, 문화기관, 의료기관, 제조기관, 자문기관 등)도 포함됨

3. 지방자치단체

① 지방자치단체는 국가영토의 일정 구역과 그 곳에 거주하는 주민을 구성원으로 하는 사단으로 일정한 범위 내의 자치권을 행사하는 법인격 있는 공공단체를 말함

- 「지방자치법」 제2조제1항제1호의 특별시, 광역시, 특별자치시, 도, 특별자치도 (광역지방자치단체)
- 「지방자치법」 제2조제1항제2호의 시, 군, 구(기초지방자치단체)
- 「지방자치법」 제2조제3항의 특별지방자치단체(지방자치단체조합)
- 「지방자치법」 제113조의 자치경찰기관, 소방기관, 교육훈련기관, 보건진료기관, 시험연구기관 및 중소기업지도기관 등의 직속기관
- 「지방자치법」 제114조의 사업소, 제115조의 출장소, 제116조의 합의제행정기관 제116조의 2의 심의회·위원회 등의 자문기관
- 「지방교육자치에 관한 법률」 제4조의 교육위원회, 제18조의 교육감
- 「지방교육자치에 관한 법률」 제34조의 하급교육행정기관 등

4. 기타 국가기관 및 공공단체 중 대통령이 정하는 기관

① 국가인권위원회법 제3조에 따른 국가인권위원회

② 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관

- 기획재정부장관이 지정하여 고시하는 기관으로 공기업, 준정부기관, 기타 공공기관으로 구분됨 (2011년 총 286개 기관)

1) 행정안전부 정부위원회 실태조사('10.4)에 근거하여 작성된 “정부위원회 현황('10.6)” 자료에서는 국가인권위원회, 진실·화해를 위한 과거사정리위원회를 중앙행정기관으로 분류하고 있으나 정부 소속이 아닌 독립기관으로 중앙행정기관 해당여부에 대해 논란이 있음



③ 특별법에 의하여 설립된 특수법인

- 출연연구기관(한국행정연구원 등), 재단(한국국제교류재단 등), 공단(한국산업인력공단 등), 진흥원, 협회, 공제조합 등으로써 국가·지자체 등으로부터의 재정 지원, 국가 또는 지자체 사무의 수탁처리, 사실상 국가 또는 지자체의 지배, 공공 또는 공익 기능 수행 등의 본질적 요소를 갖추어야 함

④ 「지방공기업법」에 따른 지방공사 및 지방공단

- 서울SH공사, 서울메트로, 경기지방공사, 지방공사 의료원 등(공사·공단 131개, 2009년)

⑤ 「초·중등교육법」 및 「고등교육법」, 그 밖의 다른 법률에 따라 설치된 각급 학교

- 초등학교, 중학교, 고등학교, 대학교, 전문대학, 방송통신대학, 기술학교, 대학원 등

Q9

개인정보보호법 적용에서 일부 제외되는 경우는 어떤 경우인가요?

공공기관이 처리하는 개인정보 중 통계법에 따라 수집되는 개인정보, 국가안전보장 관련 정보분석을 목적으로 수집 또는 제공 요청되는 개인정보, 공중위생 등 공공안전을 위해 긴급히 필요한 경우로 일시적으로 처리되는 개인정보, 언론, 종교단체, 정당이 고유목적 달성을 위하여 수집, 이용하는 개인정보 등은 개인정보보호법 제3장부터 제7장까지의 적용을 제외합니다. 또한 소상공인(5인 이하)의 경우, 내부관리계획 수립을 하지 않아도 됩니다.

※ 개인정보보호법 제58조(적용의 일부제외) ① 다음 각 호의 어느 하나에 해당하는 개인정보에 관하여는 제3장부터 제7장까지를 적용하지 아니한다.

1. 공공기관이 처리하는 개인정보 중 통계법에 따라 수집되는 개인정보
2. 국가안전보장 관련 정보분석을 목적으로 수집 또는 제공 요청되는 개인정보
3. 공중위생 등 공공안전을 위해 긴급히 필요한 경우로 일시적으로 처리되는 개인정보
4. 언론, 종교단체, 정당이 고유목적 달성을 위하여 수집, 이용하는 개인정보

※ 개인정보 안전성 확보조치 기준 고시 제3조 제2항

- ② 소상공인은 제1항에 따른 내부관리계획을 수립하지 아니할 수 있다.



Q10

동창회, 동호회 등 친목도모 단체의 적용이 일부 제외되는 조항은 몇 조 인가요?

개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조(개인정보 수집·이용), 제30조(개인정보 처리방침) 및 제31조(개인정보 보호책임자)를 적용하지 않습니다.

또한, 친목단체의 개인정보처리자에 대하여는 개인정보보호법 제75조 제1항 제1호, 제2항 제1호, 제3항 제7호 및 제8호의 벌칙을 적용하지 아니합니다. 그러나, 이외의 벌칙 규정은 친목단체의 개인정보처리자에게도 적용합니다.

※ 표준 개인정보보호지침 제66조(친목단체에 대한 벌칙조항의 적용 배제)



제2장

개인정보의 수집, 이용, 제공

Q1

홈페이지 구인게시판에 게시물 작성자가 본인의 필요에 의해서 휴대전화번호를 기재하는 경우 개인정보를 수집하게 되는 것인가요?

정보주체의 필요에 의하여 정보주체가 직접 휴대전화번호를 기재하는 것은 정보주체가 공개를 원하는 것이기 때문에 동의를 받을 필요가 없습니다.

Q2

졸업앨범에 있는 개인정보를 수집하여 전화 TM등에 활용해도 되나요?

“공개되어 있는 개인정보”라고 하더라도 당초 공개된 목적 내에서만 이용할 수 있는 것이 원칙입니다. 예컨대 졸업앨범에 개인연락처가 공개되어 있다면 동문간의 연락 등 졸업앨범 본래의 목적만을 위해 이용할 수 있으며, 회원의 동의를 얻지 않고 마케팅 행위 등에 이용하는 것은 공개된 목적 범위를 벗어나는 이용이 됩니다.

Q3

기업정보를 수집하여 활용하는 것도 개인정보보호법상 동의를 받아야 하나요?

참고로 기업의 정보(업체명, 설립년도, 사업장주소, 주요 생산품, 담당자명, 전화번호 등)를 수집하여 공공의 목적을 위해 재단법인 홈페이지에 게시되며 담당자와 담당자의 휴대전화번호는 게시되지 않습니다.

개인정보의 주체는 자연인이고 법인이나 단체에 관한 정보는 해당되지 않습니다. 따라서 기업정보 즉, 업체명, 설립연도, 사업장주소, 주요 생산품, 대표이사 또는 대표자의



성명, 임원정보 등은 개인정보로 볼 수 없습니다. 따라서 기업의 정보에 대한 동의는 필요하지 않습니다.

다만, 담당자 성명, 업무상(회사) 전화가 아닌 휴대전화 번호, 회사 이메일이 아닌 개인 이메일은 개인정보에 해당 하므로 동의가 필요합니다.

Q4

쇼핑몰에서 비회원 주문이나 게시판의 경우도 개인정보 수집동의를 받아야 한다고 하던데요. 이름과 이메일 2가지 정도만 수집하더라도 동의를 받아야 하나요?

비회원을 대상으로 게시판에서 이름과 이메일 2가지 정도만 수집하더라도 이름 및 이메일 등과 게시판에 기재된 내용 전체를 '종합적으로' 볼 때 개인을 식별할 수 있는 정도라면 개인정보입니다.

따라서 개인정보의 수집은 비회원인지 여부를 막론하고 수집 및 이용에 대한 동의를 얻어야 합니다.

Q5

신규로 직원들을 뽑을 때 이력서에 개인정보 수집 동의를 받아야 하나요?

근로자와 사용자가 근로계약을 체결하는 경우, 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의없이 개인정보를 수집·이용할 수 있습니다(표준 개인정보 보호지침 제6조 제6항). 따라서 이력서를 받는 행위는 근로계약을 체결하기 위한 준비단계로 개인정보 수집에 대한 동의는 불필요합니다.

다만, 이력서에 주민등록번호 등 고유식별정보를 수집하여 처리하는 경우에는 별도로 동의를 받아야 합니다.



Q6

만14세 미만 아동의 법정대리인을 포함한 정보주체의 동의를 받는 방법에는 어떤 것이 있나요?

정보주체의 동의를 받는 방법은 개인정보보호법 시행령 제17조에 규정되어 있습니다.

1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법
2. 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법
3. 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법
4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법
5. 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받는 방법
6. 그 밖에 제1호부터 제5호까지의 규정에 따른 방법에 준하는 방법으로 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

또한, 만 제14세 미만 아동의 법정대리인의 동의를 받는 경우 해당 아동으로부터 직접 법정대리인의 성명·연락처에 관한 정보를 수집할 수 있습니다.

Q7

병원에 방문한 만14세 미만 아동에게도 법정대리인의 동의를 받아야 하나요?

개인정보보호법 제15조 제1항 제2호는 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다고 규정하고 있습니다.

의료법 제22조에서는 진료기록부를 작성하도록 규정하고 있으며, 동법 시행규칙 제14



조에서는 진료기록부에 기재할 사항으로 “진료를 받은 자의 주소, 성명, 주민등록번호, 병력 및 가족력, 주된 증상, 진단 결과, 진료경과 및 예견, 치료내용, 진료일시분”을 규정하고 있습니다.

따라서 성인이나 만14세 미만 아동의 구분 없이 의료법에서 규정하는 개인정보는 동의 없이 수집 및 이용이 가능합니다.

Q8

병원에 내원한 환자들에 대해서 개인정보 수집 동의를 받아야 하나요?

개인정보처리자는 법률에 특별한 규정이 있거나 법령상 의무준수를 위하여 불가피한 경우에 동의 없이 개인정보를 수집·이용할 수 있습니다(개인정보 보호법 제15조 제1항 제2호).

병원의 경우 의료법 제22조 및 동법 시행규칙 제14조에 따라 진료기록부에 기재할 사항으로 “진료를 받은 자의 주소, 성명, 주민등록번호, 병력 및 가족력, 주된 증상, 진단 결과, 진료경과 및 예견, 치료내용, 진료일시분”을 명시하고 있으므로 해당되는 정보를 수집할 수 있습니다.

다만, 연락처의 경우에는 진료기록부에 기재할 사항으로 명시되어 있지 않으나 진료예약, 진단 결과의 통보 등 진료목적 범위 내에서 사용할 필요가 있을 경우에는 환자의 동의 없이 수집 가능하다고 판단됩니다.

Q9

동호회의 경우 이름과 연락처 정도 수집이 되는데 이때 모두 동의 받아야하고, 이 데이터를 컴퓨터에 저장시 암호화 해야 하나요?

개인정보보호법 제58조에 따라 동호회, 동창회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조(개인정보의 수집·이용), 제30조(개인정보 처리방침의 수립 및 공개), 제31조(개인정보 보호책임자의 지정)를 적용하지 않습니



다. 하지만 개인정보보호법의 다른 규정은 준수해야 합니다. 그리고, 개인정보보호법에서 암호화를 하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보이므로 이름 및 연락처는 암호화 대상이 아닙니다.

Q10

종교단체가 선교 목적으로 개인정보를 동의 없이 수집할 수 있나요?

개인정보보호법 제58조 제1항 제4호에 따라 종교단체가 선교를 위하여 수집·이용하는 개인정보에 대해서는 개인정보보호법 제3장부터 제7장까지의 규정을 적용하지 않습니다. 그러나 이 외의 다른 규정은 준수해야 합니다.

Q11

관공서에서 행사가 있을때 초청장을 보낼 때도 동의서를 받아야 하나요?

초청장을 보낼 때 필요한 정보(성명, 주소, 이메일 주소 등)의 수집을 정보주체로부터 직접 명함 또는 그와 유사한 매체를 제공받음으로써 한 경우, 정보주체가 동의의사를 명확히 표시하거나 그렇지 않은 경우 명함 등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있습니다.

관공서의 행사 초청장 등은 사회통념상 동의 의사가 있었다고 인정되는 범위 내로 해석되므로 별도의 동의 없이 발송해도 될 것으로 판단됩니다.

Q12

공공기관에서 개인정보를 포함하여 게시하는 경우가 있는데 이럴 경우에도 어떤 조치를 해야 하나요?

개인정보보호법 제15조 제1항에 따라 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우에는 개인정보를 수집하고 수집한 목적 내에서 이용할 수 있습니다.



다만, 개인의 사생활 침해가 되지 않도록 최소한의 범위 내에서 관계법령에 따라 게시해야 합니다.

Q13

벌과금 등 관련한 공시송달 공고를 검찰청 홈페이지 “고시/공고”란에 “성명, 징제번호, 등기번호, 수령여부” 네 가지 항목을 포함하여 게시할 경우, 개인정보보호법에 저촉되나요?

개인정보보호법 제15조 제1항 제2호에서는 “법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우”에는 개인정보를 수집하고, 그 수집 목적의 범위에서 이용할 수 있도록 규정하고 있습니다.

공시송달 공고는 형사소송법 제477조, 국제기본법 제11조에 등에 근거를 두고 있습니다만, “공시송달 공고”를 게시하는 경우, 해당 법령에 규정되어 공개토록 한 항목은 공개 가능하나 공개범위가 정해져 있지 않은 경우에는 최소한의 범위에서만 공개해야 합니다.

Q14

개인정보보호법 제15조 제2항 제4호의 내용에 “동의를 거부할 권리가 있다는 사실 및 동의의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용”을 기재하여야 한다고 했는데, 불이익 내용에 신청 또는 이용 불가라고 기재하여도 위법은 아닌가요?

동의의 거부의 경우 서비스제공이 불가능하다면 그렇게 기재할 수 있습니다만, 주의해야 할 점은 제15조 제2항 제4호를 볼 때에는 제16조 제2항을 함께 고려해야 할 것입니다.

개인정보보호법 제16조 제2항은 “개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다”고 규정하고 있습니다. 즉 선택적으로 동의할 수 있는 사항을 동의하지 아니하였다는 이유로 서비스의 제공이 거부되어서는 안 되는 것입니다.

물론 서비스이용에 필수적인 최소한의 개인정보라고 한다면, 그러한 정보의 수집에 동



의하지 않는 경우에는 불이익의 내용으로 “이용불가”라고 기재하는 것이 타당할 것입니다. 그러나 서비스이용에 불가피하게 수반되어 처리되어야 하는 개인정보가 아니라면 그러한 선택적 동의가 가능한 개인정보의 수집에 동의하지 않는다고 하여 서비스제공을 거부하면 안 될 것입니다.

Q15

개인정보보호법 제15조 제3항에 보면 “공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우”라고 되어있습니다. 여기서, 법령 등의 범위와 불가피한 경우란 무엇인가요?

공공기관이 개인정보를 수집할 수 있도록 명시적으로 허용하는 법률 규정이 없더라도, 법령 등에서 소관업무를 정하고 있고 이러한 소관업무의 수행을 위하여 불가피하게 개인정보를 수집할 수밖에 없는 경우에는 수집을 허용할 필요가 있습니다.

“법령 등”이란 법률, 시행령, 시행규칙 및 각 지방자치단체의 조례를 말합니다.

※ 예시

- 행정안전부가 「정부조직법」 제29조 및 「행정안전부와 그 소속기관 직제」, 「행정안전부와 그 소속기관 직제 시행규칙」에 따라 공무원의 인사·윤리·복무·연금 등 관리를 위해 공무원인사 관련파일을 수집·이용하거나 국가인재데이터베이스 시스템을 구축·운영하는 경우
- 국민건강보험공단이 「국민건강보험법」 제13조에 따라 보험급여관리 등을 위하여 진료내역 등을 수집·이용하는 경우

“불가피한 경우”라 함은 개인정보를 수집하지 아니하고는 공공기관의 기능과 활동을 수행할 수 없는 경우를 말합니다.

또한 불가피성의 판단은 복잡다양한 공공기관의 업무와 성격에 비추어 볼 때 법률로 규율하는 것이 불가능하므로, 일차적으로 해당 공공기관의 장이 결정하여야 합니다.



Q16

공공기관인데 감사부서나 상급기관에서 감사 목적으로 개인정보의 제공을 요청하는데 동의 없이 제공할 수 있나요?

공공감사에 관한 법률 제20조에 따르면 자체감사를 위하여 필요할 때에는 다음의 조치를 취할 수 있습니다.

1. 출석·답변의 요구(정보통신망 이용촉진 및 정보보호 등에 관한 법률에 따른 정보통신망을 이용한 요구를 포함한다)
2. 관계 서류·장부 및 물품 등의 제출 요구
3. 전산정보시스템에 입력된 자료의 조사
4. 금고·창고·장부 및 물품 등의 봉인 요구

또한, 위 조치를 요구받은 자체감사 대상기관 및 그 소속 공무원이나 직원은 정당한 사유 없으면 그 요구에 따라야 합니다.

개인정보보호법 제15조, 제17조 및 제18조에 따라 법률에 특별한 규정이 있는 경우 개인정보를 수집, 이용할 수 있으며 제3자에게 제공이 가능합니다. 또한 수집, 이용 범위를 초과하여 이용하거나 제3자에게 제공하는 것도 가능합니다.

Q17

수기로 작성된 신청서를 바탕으로 전산시스템에 등록하여 실적 등을 관리하게 되는데, 신청서에 등록에 대한 안내를 넣으면 신청서에 있는 개인정보를 전산시스템에 등록 및 활용하는 것이 가능한가요?

수기로 작성된 개인정보를 전자적으로 옮기는 경우, “개인정보파일”은 2개가 됩니다. 즉 수기파일과 전자적파일은 별개로 각각 개인정보보호법을 준수하여야 합니다.

하지만, 두 군데에서 처리되는 개인정보가 완전히 동일하고 개인정보취급방침도 같으며, 수집목적이나 이용범위 및 제3자 제공 또는 위탁처리 등이 모두 동일하다면 수기신청서에서 안내한 것을 전산시스템에 등록 및 활용하는 데 별도의 고지나 동의를 받지 않아도 될 것입니다.



Q18

종이계약서를 작성하는 사업자의 경우 계약의 이행을 위해서 주민등록번호를 수집할 경우에도 정보주체의 별도 동의가 필요하나요?

개인정보의 수집을 위한 중요한 기준은 “정보주체의 동의”입니다. 개인정보보호법 제15조 제1항 제4호의 취지는 정보주체와의 계약 체결 및 이행을 위하여 개인정보의 수집이 불가피하게 수반되는 경우에도 정보주체의 동의를 받도록 한다면, 사업자의 일상적인 영업활동에 막대한 지장을 초래할 위험이 크며 불필요한 규제가 될 수 있으므로 동의 없이도 개인정보를 수집할 수 있도록 한 것입니다. 따라서, 계약서 작성시 주민등록번호의 수집이 계약 체결 및 이행을 위하여 불가피하게 필요한 경우라고 한다면 정보주체의 동의 없이 수집이 가능합니다.

Q19

학교에서는 행사에 참여하는 학생의 사진, 학교명과 이름을 팸플릿에 넣거나 학교 홈페이지에 학생들의 생활 사진이나 행사와 관련된 사진 등을 게시하게 되는데, 개별적으로 학생들의 동의를 받아야 하나요?

학교는 공공기관으로 개인정보의 수집·이용시 법 제15조 제1항 제3호에 따라 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우 정보주체의 동의 없이 수집, 이용 가능합니다. 학생들의 정보가 학사행정에 불가피한 정보라고 한다면, 정보주체인 학생이나 또는 법정대리인의 동의(학생이 만 14세 미만일 경우) 없이 수집, 이용이 가능할 것입니다.

법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우가 아니라고 한다면 사전 동意的 필요하므로, 가급적 입학 시에 학생들이나 법정대리인의 동의(학생이 만 14세 미만일 경우)를 받는 것이 바람직합니다.



Q20

개인 블로그 등에서도 개인정보 수집이 이루어지는데 이 경우에도 동의절차 및 보호조치를 만들어야 하나요?

개인정보보호법에서 규정하는 "개인정보처리자"란 업무를 목적으로 개인정보파일을 운영하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말합니다. 따라서 개인 블로그 운영자라 할지라도 위와 같은 목적으로 개인정보를 수집하여 처리하는 경우에는 개인정보보호법의 규정을 준수하여야 합니다.

다만, 블로그 운영의 목적이 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 개인정보보호법 제58조(적용의 일부 제외) 제3항에 따라 제15조, 제30조 및 제31조를 적용하지 않습니다.

Q21

오픈 마켓에서 물건을 판매하는 업체인데, 수집할 때 별도의 동의 없이 휴대 전화번호만 받는 것도 문제가 되나요?

온라인 쇼핑물이 고객이 주문한 상품을 배송하기 위하여 주소, 연락처 정보를 수집하는 경우에는 개인정보보호법 제15조 제1항 제4호의 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 수반되는 경우에 해당됩니다. 이때에는 별도의 동의는 필요하지 않습니다. 다만, 물건을 주문하지 않은 고객의 연락처를 수집하기 위해서는 정보주체의 동의가 필요합니다.

또한 보유기간 경과 또는 수집 목적이 달성된 경우에는 즉시 파기해야 합니다.

Q22

교육접수가 중복되는 것을 방지하기 위해 접수시에는 이름, 생년월일과 성별까지만 수집을 하고, 실제 교육을 신청할 때에는 이름만 받고자 할 경우 동의가 없어도 되나요?

실제 교육을 받을 때 이름만 수집한다고 하더라도 접수 시 이미 이름, 생년월일과 성별을



수집하였기 때문에, 개인정보보호법상 특정 개인을 식별할 수 있는 정보에 해당됩니다.

그러므로 특별히 개인정보보호법 제15조 제1항 제2호부터 제6호에 해당하지 않는 한 원칙적으로 정보주체에게 제15조 제2항의 각호 내용을 알리고 동의를 받아서 수집해야 할 것입니다.

Q23

개인정보를 제3자에게 제공할 수 있는 방법이 있나요?

개인정보보호법 제17조 제1항에 따라 개인정보처리자가 개인정보를 수집한 목적 범위 내에서 제3자에게 제공할 수 있는 경우는 다음과 같습니다.

1. 정보주체의 동의를 받은 경우(제3자 제공시 고지하고 동의 받을 내용 : ①제공받는 자, ②제공받는 자의 이용목적, ③제공하는 개인정보 항목, ④개인정보를 제공받는 자의 보유 및 이용기간, ⑤동의거부 권리 및 동의 거부시 불이익의 내용)
2. 법률의 특별한 규정, 법령상 의무 준수를 위해 불가피한 경우, 공공기관이 법령에서 정한 소관업무 수행을 위해 불가피한 경우, 정보주체 등의 생명, 신체, 재산의 이익 보호를 위해 개인정보를 수집한 목적범위 내에서 개인정보를 제공하는 경우

또한 개인정보보호법 제18조 제2항에 따라 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있습니다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정됩니다.

1. 정보주체의 동의를 받은 경우(제3자 제공시 고지하고 동의 받을 내용 : ①제공받는 자, ②제공받는 자의 이용목적, ③제공하는 개인정보 항목, ④개인정보를 제공받는 자의 보유 및 이용기간, ⑤동의거부 권리 및 동의 거부시 불이익의 내용)
2. 다른 법률에 특별한 규정이 있는 경우
3. 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

4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정한 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정보 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

Q24

자체 수집한 정보가 아니고 다른 기관에서 입수한(제공받은) 자료도 활용이 가능한가요?

개인정보를 타 기관으로부터 제공받아 이용하고자 하는 경우 원칙적으로 개인정보보호법 제17조 제1항 제1호에 따라 정보제공을 하는 측에서 정보주체로부터 개인정보의 제3자 제공에 대해 별도의 동의를 받아야 합니다.

다만, 개인정보보호법 제17조 제1항 제2호에 따라 타기관이 제15조 제1항 제2호·제3호 및 제5호에 따라 수집한 개인정보를 목적 범위에서 제공했거나, 제18조 제2항 제2호 내지 제9호에 의거하여 개인정보를 제공했다면 별도의 동의를 받지 않고도 개인정보를 제3자에게 제공하고 제공받은 자는 제공받은 목적 범위 내에서만 이용할 수 있습니다.

Q25

개인정보 처리업무 위탁에 대한 원칙 및 방법은 무엇인가요?

〈개인정보 처리업무 위탁의 원칙〉

제3자에게 개인정보 처리업무 위탁은 문서에 의하여야 합니다. 위탁문서에는 ①위탁업



무 수행목적 외의 개인정보 처리금지, ②기술적·관리적 보호조치, ③위탁사무 목적 및 범위, ④재위탁 제한, ⑤위탁업무와 관련하여 보유하는 개인정보의 관리현황 점검 감독, ⑥수탁자의 의무 위반시 손해배상의 내용이 포함되어야 합니다.

또한 개인정보처리자는 위탁사실을 정보주체가 쉽게 확인할 수 있도록 ①위탁하는 업무의 내용, ②개인정보 처리업무를 위탁받아 처리하는 자(수탁자)를 공개해야 합니다.

〈개인정보 처리업무 위탁의 방법〉

위탁자는 자신의 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재하여야 합니다. 인터넷 홈페이지 게재가 불가능할 때에는 ①위탁자 사업장 등의 보기 쉬운 장소에 게시, ②관보, 신문 게재, ③연 2회 이상 발행하는 간행물, 소식지 등에 게재, ④재화용역을 제공하기 위해 작성한 계약서에 게재하여 발급하는 방법 등의 하나 이상을 사용할 수 있습니다.

Q26

내부 직원에 대한 교육을 외부 업체에 위탁할 때 위탁에 대한 동의를 받아야 하나요?

표준 개인정보 보호지침에서는 근로자와 사용자가 근로계약을 체결하는 경우, 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의없이 개인정보를 수집·이용할 수 있도록 규정하고 있습니다. 따라서 내부 직원에 대한 교육 위탁은 별도 동의는 필요하지 않지만 위탁내용과 수탁자를 고지해야 합니다.

Q27

재개발을 하기 위하여 주민자치회에서 주민들의 의견을 수렴하기 위해 기존에 수집한 개인정보(이름, 주민등록번호, 주소, 전화번호)를 이용하여 우편물을 발송해도 되나요?

개인정보는 개인정보보호법 제18조 제2항의 각호에 규정된 경우 외에는 수집목적의 범위 내에서만 이용할 수 있습니다. 동대표나 주민자치회가 적법하게 수집한 개인정보를 수집 목적의 범위 내에서 이용하는 것은 문제가 없습니다.



그러나 적법하게 수집하지 않은 정보이거나, 적법하게 수집된 정보라도 수집 목적이 다르다면 정보주체의 동의를 받아야 합니다.

Q28

퇴사한 직원에 대한 근무기록 등은 퇴사 후 몇 년간 보관하면 되나요?

근로기준법 시행령 제19조(사용증명서의 청구)에 따르면, 법 제39조 제1항에 따라 사용증명서를 청구할 수 있는 기한은 퇴직 후 3년 이내로 하고 있습니다. 이는 3년간만 보관하라는 의미가 아니라, 최소한 3년간은 반드시 보관하고 그 이상을 보관하기 위해서는 정보주체의 동의 등 별도의 절차가 필요한 것으로 판단됩니다. 따라서, 입사시에 경력증명서 발급 등을 위하여 필요한 개인정보를 퇴직 후 몇 년간 보관하게 된다는 내용을 별도로 고지하고 동의를 받아 두는 것이 바람직하다고 판단됩니다.

Q29

채용을 위해서 개인정보를 수집하고 퇴직하고 나서 개인정보를 20년 동안 보유한다는 것에 동의를 받으면 문제가 없나요?

표준개인정보보호지침 제6조 제6항에 따르면 근로계약을 체결하는 경우 근로기준법 제2조제5호의 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의 없이 개인정보를 수집·이용할 수 있습니다.

개인정보의 보유기간에 대하여는 법령에서 별다른 규정은 없습니다. 따라서 합리적인 범위 내에서 보유기간을 산정하고 이를 고지, 동의 받는다면 법 위반은 아니라고 판단됩니다.

다만, 보유기간에 대한 입증책임, 즉 보유를 해야 하는 필수기간에 대한 입증책임은 사업자에게 있습니다.



Q30

개인정보수집동의서를 받아서 처리할 경우 동의서 내용에 보유 및 이용기간은 개인정보처리자의 필요에 의해 보유기간을 정하면 되는 건가요?

개별 법령에 구체적인 보유기간이 명시되어 있지 않은 경우에는 개인정보 보호책임자의 협의를 거쳐 기관장의 결재를 통하여 결정해야 합니다. 다만, 보유기간은 별표 1의 개인정보파일 보유기간 책정 기준표에서 제시한 기준과 공공기록물 관리에 관한 법률 시행령에 따른 기록관리기준표를 상회할 수 없습니다.

〈개인정보파일 보유기간 책정 기준표〉

보유기간	대상 개인정보파일
영구	1. 국민의 지위, 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일 2. 국민의 건강증진과 관련된 업무를 수행하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일
준영구	1. 국민의 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 개인이 사망, 폐지 그 밖의 사유로 소멸되기 때문에 영구 보존할 필요가 없는 개인정보파일 2. 국민의 신분증명 및 의무부과, 특정대상 관리 등을 위하여 행정기관이 구축하여 운영하는 행정정보시스템의 데이터 셋으로 구성된 개인정보파일
30년	1. 관계 법령에 따라 10년이상 30년 미만의 기간 동안 민·형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
10년	1. 관계 법령에 따라 5년이상 10년 미만의 기간 동안 민·형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
5년	1. 관계 법령에 따라 3년이상 5년 미만의 기간 동안 민·형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
3년	1. 행정업무의 참고 또는 사실 증명을 위하여 1년 이상 3년 미만의 기간동안 보존할 필요가 있는 개인정보파일 2. 관계 법령에 따라 1년이상 3년 미만의 기간 동안 민·형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 3. 각종 증명서 발급과 관련된 개인정보파일(단 다른 법령에서 증명서 발급 관련 보유기간이 별도로 규정된 경우 해당 법령에 따름)
1년	1. 상급기관(부서)의 요구에 따라 단순 보고를 위해 생성한 개인정보파일



Q31

서비스 계약과 관련하여 개인정보 보유기간 설정을 어떻게 해야 하나요?

개별 서비스 계약의 특성에 따라 보유기간을 설정하면 됩니다. 만일 특별한 법(예를 들어 전자상거래소비자보호법 등)에서 정한 기간이 있다면 해당 법률의 정해진 기간에 따라 보유 가능합니다.

Q32

개인정보의 파기 시기 및 방법은 어떻게 되나요?

개인정보는 보유기간의 경과, 개인정보 처리목적 달성 등 개인정보가 불필요하게 되었을 때에는 지체 없이(5일 이내) 파기해야 합니다. 다만, 다른 법령에 따라 보존해야 하는 경우에는 보관할 수 있습니다. 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 해야 합니다. 종이에 출력된 개인정보나 가입신청서 등 개인정보가 기재된 문서는 분쇄기로 분쇄하거나 소각해야 합니다.

전자적 파일 형태는 복원이 불가능한 방법(사회통념상 현재 기술 수준에서 적절한 비용이 소요되는 방법)으로 영구 삭제해야 합니다. 예를 들면, 하드디스크에 기록된 정보를 삭제할 때에는 데이터 복원을 방지하기 위해 ‘로우레벨포맷’ 명령으로 포맷을 하거나, 일반 포맷을 한 뒤 불필요한 정보를 여러 번 덮어쓰우는 방법으로 다시는 재생할 수 없도록 조치해야 합니다.

Q33

개인정보 파기 시 예외 경우가 있나요?

개인정보보호법 제21조 및 시행령 제16조에 따라, 다른 법령에 따라 보존하여야 하는 경우 외에는 개인정보가 불필요하게 되었을 때에는 지체 없이 파기해야 합니다.



Q34

쇼핑몰에서 탈퇴한 회원들의 개인정보를 파기하려고 하는데, 일부 회원들은 할부 요금이 아직 미납되었거나 제품 A/S 기간이 남아있습니다. 이러한 경우에는 어떻게 해야 하나요?

사업자는 개인정보의 수집·이용 목적이 달성된 경우 등에는 지체없이 개인정보를 파기하여야 하나, 예외적으로 “다른 법률에 따라 개인정보를 보존하여야 하는 경우”에는 개인정보를 파기하지 않고 보존할 수 있습니다.

예를 들어, 전자상거래 등에서의 소비자 보호에 관한 법률 및 동법 시행령에서는 대금 결제 및 재화 공급에 관한 기록을 5년간 보관하도록 하고 있으므로, 질의와 같이 요금 미납, A/S 등에 해당하는 경우에는 동법에 의거 5년간 개인정보 보관이 가능합니다.

Q35

개인정보를 정정·삭제 요청할 수 없는 경우도 있나요?

개인정보보호법 제4조 제4호는 정보주체의 권리 중 하나로 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리를 규정하고 있습니다. 하지만 개인정보보호법 제36조에 의거하여 개인정보 삭제요청이 불가한 경우도 있을 수 있습니다. 법령에 의하여 개인정보를 수집·보관해야 할 의무가 있는 경우, 정보주체의 요구만으로 해당 개인정보를 삭제하면 법령의 목적 달성이 곤란할 수 있기 때문입니다.

※ 개인정보보호법 제36조(개인정보의 정정·삭제) ① 제35조에 따라 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다.



제3장

개인정보의 처리

가. 민감정보의 처리제한

Q1

개인의료정보(or 개인건강정보) 중 “개인을 알아볼 수 있는 정보”가 개인정보 인가요? 아니면 개인의료정보(or 개인건강정보) 전체가 개인정보 인가요?

의료정보의 개인정보 포함여부는 정보조합으로 개인식별이 가능한지 여부가 기준이 되며, 포함관계가 확실적으로 정해지는 것은 아닙니다. 예를 들어 이름, 주민등록번호 등과 같이 개인을 식별할 수 있는 정보가 의료정보와 함께 시스템에 저장되면 개인정보에 해당하나, 특정인을 식별할 수 없게 시스템에 저장되면 개인정보로 보지 않습니다.

Q2

환자로부터 수집하지 않고 각 의료기관에서 자체 발급하는 병록번호는 개인정보 인가요? 그리고 병록번호에 연결된 건강정보는 개인정보 인가요?

개인정보 여부는 식별가능성으로 판단되며, 환자 고유번호, 병록번호(일명 차트번호-의무기록 차트에 붙는 고유번호) 그 자체로는 개인정보라 하기 어려울 수 있으나, 이름과 같이 개인을 식별할 수 있는 연계정보를 같이 시스템에 저장한다면 개인정보에 해당합니다.



Q3

개인정보보호법 제15조(개인정보의 수집·이용)에서 의료기관의 개인정보정보(개인건강정보) 수집은 동의 대상인가요?

의료기관에서 의료법에 근거하여 수집하는 개인정보는 개인정보보호법 제15조 제1항 제2호의 '법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우' 및 제4호의 '정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우'에 해당되어 동의없이 수집할 수 있습니다.

다만, 의료법에서 요구하는 이외의 사항을 수집하는 경우에는 별도의 정보주체 동의가 필요합니다만, 연락처의 경우에는 진료기록부에 기재할 사항으로 명시되어 있지 않으나 진료예약, 진단 결과의 통보 등 진료목적 범위 내에서 사용할 필요가 있을 경우에는 환자의 동의 없이 수집 가능하다고 판단됩니다.

※ 의료법 시행규칙 제14조(진료기록부 등의 기재 사항)

1. 진료기록부

- 가. 진료를 받은 자의 주소·성명·주민등록번호·병력(病歷) 및 가족력(家族歷)
- 나. 주된 증상, 진단 결과, 진료경과 및 예견
- 다. 치료내용(주사·투약·처치 등)
- 라. 진료 일시분(日時分)

Q4

개인정보보호법 제23조(민감정보의 처리 제한)에서 건강, 성생활을 민감정보로 정의하고 처리하지 말 것을 규정하고 있는데, 병원에서 건강정보를 수집할 수 있나요?

의료기관에서 의료법에 근거하여 수집하는 민감정보는 개인정보보호법 제23조(민감정보의 처리 제한)의 제2호 "법령에서 민감정보의 처리를 요구하거나 허용하는 경우"에 해당하므로 별도의 동의 없이 처리할 수 있습니다. 다만, 법에서 요구하는 이외의 사항을 수집하는 경우에는 정보주체의 별도 동의가 필요합니다.



Q5

신규 환자가 아닌 기존 환자에 대한 동의는 어떻게 받아야 하나요?

법 시행 이전에 수집한 환자의 개인정보는 별도의 동의가 필요하지 않습니다. 개인정보 보호법 부칙 제4조(처리중인 개인정보에 관한 경과조치), 표준지침 제67조(처리 중인 개인정보에 관한 경과조치) 규정에 따라 기존에 수집한 개인정보는 수집목적 범위 내에서 보유·이용할 경우, 별도의 동의가 필요하지 않습니다.

나. 고유식별정보의 처리제한

Q1

홈페이지를 통하여 주민등록번호를 수집하는 경우 정보주체에게 별도 동의를 받으라고 하는데 별도 동의 받는 적절한 방법에는 무엇이 있나요?

고유식별정보를 처리하기 위해서는 다른 개인정보의 처리에 대한 동의와는 별도로 동의를 받아야 합니다. 즉, 동의 받는 항목에 고유식별정보의 처리에 대한 별도의 항목을 만들어 동의를 받아야 합니다.

동의를 받는 방법은 다음과 같습니다(시행령 제17조)

1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법
2. 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법
3. 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷주소 등을 통하여 동의 사항을 확인한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법
4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법



Q2

기존 주민등록번호를 “111111-1xxxxxx”로 변환하여 보유하려 하는데 이러한 데이터가 개인정보보호법에서 규정하고 있는 고유식별정보에 해당이 되나요?

주민등록번호는 13자리가 모두 있어야 주민등록번호로서 개인을 식별할 수 있는 기능을 한다고 보는 것이 타당합니다. 따라서 생년월일과 성별(123456-1*****)까지만 수집·보유하고 있는 것은 개인정보보호법에서 말하는 “고유식별정보”로 보기 어렵습니다.

다만, 수집 당시는 생년월일과 성별(123456-1*****)에 대한 정보가 아닌, 주민등록번호를 수집하고 그 수집된 주민등록번호를 이용하여 생년월일과 성별(123456-1*****)로 처리를 한다면 고유식별정보의 수집 및 처리에 해당합니다.

Q3

기존에 가지고 있던 주민등록번호는 폐기해야 하나요? 아니면, 전체 회원에 대해 다시 동의 절차를 받아야 하나요?

개인정보보호법 부칙 제4조, 표준 개인정보 보호지침 제67조(처리중인 개인정보에 관한 경과조치)에 따라 개인정보보호법 시행 전에 다른 법령에 따라 적법하게 처리된 개인정보는 개인정보보호법에 따라 적법하게 처리된 것으로 보고 있습니다.

즉, 법 시행 전에 근거법령 없이 개인정보를 수집한 경우 당해 개인정보를 보유하는 것은 적법한 처리로 보지만, 법 시행 이후 기존의 수집목적 범위를 벗어나 이용하는 경우에는 개인정보보호법, 시행령, 시행규칙 및 표준 지침을 준수해야 합니다.

따라서, 기존에 가지고 있던 주민등록번호를 보유하는 것은 적법하지만, 기존 수집 목적 범위 내를 벗어나 처리를 해야 할 경우에는 별도의 동의 절차 등 법령을 준수해야 합니다. 또한 주민번호 등 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 합니다(법 제24조 제3항).



Q4

사원증 번호, 회원번호 등 개인에게 고유하게 부여되는 번호도 고유식별정보의 범위에 포함되나요?

고유식별정보란 법령에 따라 개인의 고유한 특성을 구별하기 위하여 부여된 식별정보로서 대통령이 정하는 정보만을 의미합니다. 개인정보보호법 시행령에서 정하고 있는 고유식별정보는 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호입니다.

Q5

여권판독기로 여권정보를 확인하여 고객의 호텔 예약을 확인하고 있는데 개인정보보호법에 위반이 되나요?

여권판독기로 여권정보를 판독할 경우 여권번호 등 개인정보를 처리하는 것으로 볼 수 있습니다. 여권번호는 고유식별정보로 정보주체에게 별도로 동의를 받거나 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우에 한하여 처리할 수 있습니다(개인정보보호법 제24조 제1항).

Q6

주민등록번호 대체수단 의무도입은 어떤 경우에 해야 하나요?

주민등록번호 외의 회원가입방법 제공의무자는 공공기관 또는 공공기관 외에 인터넷 홈페이지를 운영하는 개인정보처리자로서 전년도 말 기준 직전 3개월간 그 인터넷 홈페이지를 이용한 정보주체의 수가 하루 평균 1만명 이상인 경우에 해당합니다.

Q7

건물 출입시에 신분확인하고 출입증 교부를 위해서 성명을 적고 신분증을 받아 기록하고 보관하는 경우 개인정보 및 고유식별정보 수집·이용 동의서를 받아야 하나요?

출입증 교부시 고유식별정보가 포함되어 있는 신분증을 기록·보관하는 경우 고유식별



정보를 수집하는 것으로 볼 수 있습니다.

따라서 개인정보보호법 제15조 제2항에 따라 ①개인정보의 수집·이용 목적, ②수집하려는 개인정보의 항목, ③개인정보의 보유 및 이용 기간, ④동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 등에 대하여 정보주체에게 알리고 동의를 받아야 합니다.

또한 고유식별정보를 수집하므로 고유식별정보의 처리에 대하여는 별도의 동의를 추가적으로 받아야 합니다.

Q8

병원의 경우 주민등록번호 수집 이용이 필수인데 주민등록번호 대체 수단 마련이 의무화되나요?

주민등록번호 외의 회원가입방법 제공의무자는 공공기관 또는 공공기관 외에 인터넷 홈페이지를 운영하는 개인정보처리자로서 전년도 말 기준 직전 3개월간 그 인터넷 홈페이지를 이용한 정보주체의 수가 하루 평균 1만 명 이상인 경우에 해당합니다. 즉, 홈페이지를 통하여 회원으로 가입할 경우에 해당하는 사항입니다.

Q9

읍·면·동에서 민원인이 공공 아이핀을 신청하는 업무가 있습니다. 만일 14세 미만 아동이 공공 아이핀을 신청하는 경우 법정 대리인과 동행하여 신청해야 하는지요?

공공 아이핀 발급신청을 할 경우, 미성년자는 법정대리인(부모님 등)과 함께 방문해야 합니다. 해당 내용은 공공기관 아이핀 안내 홈페이지(<http://www.g-pin.go.kr> → 방문신청 발급 안내)에 설명되어 있습니다.



다. 영상정보처리기기의 설치·운영 제한

Q1

사람을 촬영하지 않아 개인정보 침해 위험이 전혀 없는(안개, 황사 등의 기상 상황 파악) 영상정보처리기기에 대하여 개인정보보호법이 적용되나요?

개인정보보호법 제2조 제7항에서 정의하고 있는 영상정보처리기기란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 폐쇄회로 텔레비전과 네트워크 카메라를 말합니다.

여기에서 '사물'이란 개인정보보호법의 입법취지를 고려할 때, 이 법의 보호대상이 되는 사람과 일정한 관계가 있는 사물로 한정하여 해석이 됩니다. 이와 같이 개인정보보호법의 취지가 개인정보의 수집·유출·오용·남용으로부터 사람의 사생활의 비밀 등을 보호하기 위한 것이므로, 사람과 연계되지 않아 개인정보침해가 발생할 여지가 없는 사물의 촬영을 위한 영상정보처리기기에 대해서는 개인정보보호법이 적용되지 않습니다.

예를 들어 천문대에 설치된 망원경은 비록 일정한 공간에 지속 설치되어 우주공간(사물)을 촬영하고는 있으나 그 촬영대상이 사람과 일정한 생활관계에 놓여져 있다고 보기 어렵기 때문에, 이 법에 따른 영상정보처리기기에 포함되지 않습니다.

따라서 사람을 촬영하지 않는 안개, 황사 등의 기상상황 파악 등을 목적으로 하는 영상정보처리기기는 개인정보보호법의 적용을 받지 않는다고 판단됩니다.

Q2

영상정보처리기기(CCTV)는 어떤 경우에 설치할 수 있나요?

영상정보처리기기는 공개된 장소에 특정 목적(①법령에서 구체적으로 허용하는 경우, ②범죄예방 및 수사, ③시설안전 및 화재예방, ④교통단속, ⑤교통정보의 수집, 분석 및 제공)으로만 설치·운영할 수 있습니다.



목욕실, 화장실, 탈의실 등 개인 사생활을 현저히 침해할 우려가 있는 장소에는 영상정보처리기기를 설치·운영할 수 없습니다(다만 교정시설, 정신의료기관에는 설치·운영 허용).

영상정보처리기기는 설치목적과 다른 목적으로 영상정보처리기기를 임의 조작, 다른 곳을 비추는 행위, 녹음기능 사용을 할 수 없습니다.

영상정보처리기기를 설치·운영할 때에는 설치목적 및 장소, 촬영범위 및 시간, 관리책임자 및 연락처 등이 기재된 안내판을 정보주체가 쉽게 인식할 수 있도록 설치해야 합니다.

건물 안에 다수의 영상정보처리기기 설치시, 출입구 등 잘 보이는 곳에 해당 시설·장소 전체가 설치지역임을 표시하는 안내판을 설치할 수 있습니다.

또한, 공공기관이 원거리 촬영, 과속, 신호위반단속 등을 목적으로 설치하는 경우, 장소적 특성으로 안내판 설치가 불가능하거나 설치하더라도 정보주체가 쉽게 알아볼 수 없는 경우에는 인터넷 홈페이지에 기재사항을 게재하는 것으로 안내판 설치에 갈음할 수 있습니다.

Q3

CCTV를 목욕탕 휴게실, 수면실 등에 설치할 수 있나요?

개인정보보호법 제25조제1항은 ①법령에서 구체적으로 허용하고 있는 경우, ②범죄의 예방 및 수사를 위하여 필요한 경우, ③시설안전 및 화재 예방을 위하여 필요한 경우, ④교통단속을 위하여 필요한 경우, ⑤교통정보의 수집·분석 및 제공을 위하여 필요한 경우를 제외하고는 공개된 장소에 CCTV를 설치·운영하는 것을 금지하고 있습니다.

그러나 개인정보보호법 제25조 제1항 제1호 및 공공위생관리법 시행규칙 별표1에 따라 목욕장업자는 목욕실, 발한실, 탈의실 이외의 시설에 무인감시카메라를 설치할 수 있습니다.

다만, 수면실이나 휴게실이라 하더라도 탈의한 상태로 다니는 곳은 CCTV를 설치할 수 없습니다.



Q4

직장에서 작업감시를 위해 CCTV를 설치하려면 어떤 기준에 따라야 하는지요?

직장 등 근로 공간에 설치된 영상정보처리기기는 사용자 측의 근로 관리권한과 근로자 측의 사생활 보호권이 서로 상충될 우려가 있습니다. 외부인의 출입이 통제되는 근로공간은 원칙적으로 '비공개된 장소'에 해당하므로 이 법 제25조는 적용되지 않으며, 그 외의 일반적 개인정보보호 원칙의 적용을 받습니다.

이와 관련하여, 근로자참여 및 협력증진에 관한 법률에서는 CCTV와 같은 근로자감시장비는 노사 양자의 협의사항으로 규정하고 있으므로, 근로 모니터링 목적의 CCTV 설치 범위 및 사생활 침해 방지조치 등을 노사 협의에 따라 정하여 설치·운영할 수 있습니다.

Q5

CCTV를 따로 녹화하지는 않고 관찰만 하고 있는데 이런 경우에도 개인정보 보호법에 해당이 되나요?

CCTV 녹화와는 상관없이 CCTV를 설치·운영하고 있다면 개인정보보호법 제25조에 따라 개인정보보호법의 규정을 준수해야 합니다.

Q6

버스회사에서 폭행사건, 범죄예방 등을 파악하기 위해 CCTV 녹음기능을 사용하고 싶은데 가능한가요?

영상정보처리기기운영자는 영상정보처리기기에서 녹음기능을 사용할 수 없습니다(법 제25조 제5항). 그러므로 영상정보처리기기에서 녹음기능을 사용하는 것은 원칙적으로 위법하게 됩니다.



Q7

개인정보보호법 제25조에 따라 공개된 장소에 설치되는 영상정보처리기에 대하여 적용이 일부 제외되는 조항은 어떤 것이 있나요?

영상정보처리기는 개인정보보호법의 다음 각 조항에 대해 적용이 제외됩니다.

- ① 제15조(개인정보 수집·이용)
- ② 제22조(동의를 받는 방법)
- ③ 제27조(영업양도시 개인정보 이전제한)
- ④ 제34조(개인정보 유출통지)
- ⑤ 제37조(처리정지)

Q8

건물 밖에 여러 대의 CCTV가 설치되어 있는 경우 안내판을 각각 설치해야 하나요?

표준 개인정보보호지침 제43조 제2항에 따라 영상정보처리기 운영자가 안내판의 크기, 설치위치 등을 자율적으로 정할 수 있습니다.

다만, 정보주체가 알아보기 쉬운 장소에 누구라도 용이하게 관독할 수 있도록 설치되어야 합니다.

Q9

개인정보보호법상 운영 중인 영상정보처리기에 목적을 추가할 경우 어떤 절차를 거쳐야 하나요?

과거에는 지방자치단체의 CCTV운영 규정에 따라 행정안전부장관과 협의를 해야 하지만, 개인정보보호법에서는 사전 의견수렴 및 안내판 수정(목적추가)을 하면 됩니다.



Q10

영상정보처리기기를 다목적용(시설안전, 주차관리, 범죄예방 등)으로 이용하고 통합관리 하는 경우 안내판에 “다목적용”이라고 표기하면 되나요?

안내판에는 목적을 모두 명시하여야 하고, 표준 개인정보보호지침에 따라 통합 시스템 관리에 관한 사항을 추가로 명시하여야 합니다. 따라서 '다목적용'과 같은 표현보다는 모든 목적을 다 명시하는 것이 개인정보보호법의 취지에 맞습니다.

라. 업무위탁에 따른 개인정보의 처리제한

Q1

사업자가 고객의 DM발송을 타 업체에 위탁할 경우 동의가 필요한가요?

개인정보보호법 제26조 제3항에 의하면 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법(서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법)에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 합니다.

따라서, 고객의 DM 발송을 타 업체에 위탁하는 경우 개인정보보호법 제26조 제3항에 따라 정보주체에게 고지하는 것으로 충분할 것입니다.

Q2

포인트 카드사와 제휴를 맺어 결제시 포인트로 결제할 수 있도록 하려면 어떻게 해야 하나요?

포인트 카드사가 포인트 적립 및 결제 업무만 대행하는 수탁자라고 한다면, 이는 개인정보 위탁에 해당되어 위탁자 및 수탁자는 개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리 제한) 규정을 준수해야 합니다.

만일, 제휴 맺은 포인트 카드사가 제공받은 개인정보로 카드사의 이익이나 목적을 위해



사용하는 형태라고 한다면, 이는 개인정보 제3자 제공에 해당되어, 정보주체에게 개인 정보를 제공받는 자, 제공항목, 제공받는 자의 이용목적, 보유·이용기간을 고지한 후 정보주체로부터 별도의 동의를 획득하여야 합니다.

Q3

외국계 회사로 내부인사시스템의 관리는 외국의 본사에서 관리하고, 직원들의 개인정보는 한국지사를 거쳐 외국의 본사로 전달이 되며, 외국본사는 다시 외국의 타 회사에 관리업무를 위탁하여 처리를 하고 있습니다. 이 경우 직원들의 동의를 받아야 하나요?

개인정보보호법 제17조 제3항에 따라 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항의 각 호에 따른 사항 즉, ①제공받는 자, ②제공받는 자의 이용목적, ③제공하는 개인정보 항목, ④개인정보를 제공받는 자의 보유 및 이용기간, ⑤동의거부 권리 및 동의 거부시 불이익의 내용을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결해서는 안됩니다.

Q4

고객만족도 조사를 위해 이름과 전화번호를 위탁업체에 제공하게 되는데 이 경우 동의를 받아야 하나요?

설문조사 기관에 개인정보의 처리를 위탁하는 경우 정보를 제공하는 자가 개인정보처리자(위탁자)가 되고 조사업체는 수탁자가 되는 관계에 놓이게 됩니다.

그리고 제3자 제공과는 달리 개인정보보호법상 위탁에 대해서는 정보주체로부터 별도로 동의를 받지 않아도 되는 것이므로, 개인정보보호법 제26조를 참조하여 위탁내용을 고지하시고 설문조사를 행하면 될 것입니다.



제4장

개인정보의 안전한 관리

가. 안전조치 의무

Q1

개인정보의 안전성 확보조치는 무엇인가요?

개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 다 음과 같은 기술적·관리적 및 물리적 조치를 강구해야 합니다.

1. 관리적 조치 : 내부관리계획의 수립 및 시행, 교육계획 수립 및 실시, 기록물의 관리 및 보호조치, 정기적인 자체 감사의 실시, 보호(보안)구역 지정 등
2. 물리적 조치 : 출입통제 장치 설치, 물리적 잠금장치 설치, 감시장치 설치 등
3. 기술적 조치 : 시스템 접근권한 관리, 접근권한 확인(식별, 인증 등), 침입차단, 방지 시스템 설치, 고유식별정보의 암호화, 접속기록의 위변조 방지, 보안프로그램의 설 치, 주기적인 S/W업데이트 및 점검 등

Q2

소기업 및 소상공인 지원을 위한 특별조치법에 따른 소상공인입니다. 내부관리 계획을 수립하지 않아도 되나요?

소상공인은 “개인정보의 안전성 확보조치 기준” 제3조 제2항에 의거 내부관리계획을 수립하지 않아도 됩니다.



Q3

내부 직원의 인사정보와 외부 전문가 정보 등의 DB를 관리하고 있습니다. 개인 정보보호법에 따라서 별도의 안전장치를 해야 하나요?

개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 합니다(개인정보보호법 제29조).

따라서 개인정보를 직접 취급하는 직원 등에 의한 내부자 유출 등을 방지하기 위하여 내부관리계획의 수립·시행, 직원 교육 실시, 전산실·자료보관실 보안구역 설명 및 출입통제, 단말기의 지령·관리 및 접근 권한 제한, 접속기록 보관 및 위·변조 방지 등의 조치를 취해야 합니다.

Q4

이전에 수집한 개인정보도 모두 암호화해야 하나요?

개인정보보호법 시행령 제25조 및 제33조에 따라 암호화해야 하는 개인정보는 고유식별정보, 비밀정보 및 바이오정보를 말합니다.

법 시행전(11.9.30)에 수집·보유하고 있는 개인정보 암호화는 '12년 12월 31일까지 유예기간을 부여하고 있으므로, 법 시행 전에 수집한 개인정보 중 고유식별정보, 비밀정보, 바이오정보가 있다면 '12년 12월 31일까지 암호화조치를 하여야 합니다.

다만, 개인정보의 안전성 확보조치 기준 제7조 제2항에 따라 내부 망에서 송·수신되는 고유식별정보는 업무상 필요할 경우 암호화 대상에서 제외할 수 있으나, 비밀번호와 바이오정보는 반드시 암호화하여야 합니다.

만일, 전용선을 이용하여 개인정보를 송·수신하는 경우, 암호화가 필수는 아니나 내부자에 의한 개인정보 유출 등을 대비해서 가급적 암호화 전송을 권장하고 있습니다.

개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 개인정보 영향평가 및 위험도 분석결과에 따라 암호화 적용여부 및 적용범위를 결정하여 시행할 수 있습니다.



즉, 시행령 제38조에 따라 영향평가의 대상이 되는 공공기관은 해당 개인정보 영향평가의 결과에 따라 암호화의 적용여부 및 적용범위를 정하여야 하며, 개인정보 영향평가의 실시대상이 아니거나 공공기관 이외의 개인정보처리자는 위험도 분석을 실시한 후 그 결과에 따라 고유식별정보의 암호화 적용여부 및 적용범위를 정하여 시행합니다.

- ※ “고유식별정보”는 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며, 대통령령으로 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호입니다.
- ※ “비밀번호”는 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말합니다.
- ※ “바이오정보”는 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함합니다.

Q5

주민등록번호를 저장하면 무조건 암호화해야 하나요?

아닙니다. 필요성 판단 후 암호화 합니다. 인터넷에서 직접 접근이 가능한 구간(인터넷 망, DMZ 구간)에 위치한 시스템에 저장하면 암호화해야 하나, 물리적인 망분리, 방화벽 등으로 분리된 내부망에 저장하면 개인정보 영향평가나 위험도 분석을 통해 필요한 경우에만 암호화를 합니다.

Q6

국내에 있는 직원의 DB가 해외 시스템에 있는데 암호화를 해야 하나요?

해외 시스템에 DB가 있다고 하더라도 국내의 법률을 준수하여야 합니다. 따라서 개인정보제공자 및 수신자, 수신한 자료부터 개인정보를 재차 수령한 제2의 개인정보처리자는 개인정보가 이전되는 과정 또는 이전된 이후 개인정보가 불법열람, 유출 등 침해가 발생되지 않도록 적절한 수준의 기술적·관리적 안전성 확보조치를 취하여야 합니다.



Q7

비디오대여점에서 고객관리를 위해 업무용 컴퓨터를 운영하고 있는데, “개인 정보의 안전성 확보조치 기준”에 따라 어떠한 조치가 필요한가요?

업무용컴퓨터로 고객정보를 관리하시는 경우 제5조(비밀번호 관리)에 따라 업무용컴퓨터에 비밀번호를 설정하시고 업무용컴퓨터에서 제공되는 침입차단기능을 설정하셔야 하며 악성프로그램을 차단하도록 백신프로그램을 설치하셔야 합니다.

또한 업무용컴퓨터에 주민등록번호 등 고유식별정보가 저장된 경우에는 암호화 등의 보안조치를 수행하셔야 합니다.

Q8

백화점에서 고객정보 데이터베이스를 운영하고 있습니다. 개인정보 암호화 대상이 무엇이며 어떻게 해야 하나요?

개인정보보호법 상에서 요구되는 암호화 대상은 고유식별정보(주민등록번호, 외국인등록번호, 운전면허번호, 여권번호), 비밀번호, 바이오정보입니다. 개인정보처리자는 고유식별정보 등을 정보통신망 또는 보조기억매체 등을 통해 전달하는 경우 암호화하여 전송해야 합니다.

인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 고유식별정보를 저장하는 경우에도 반드시 암호화하여야 합니다. 또한 내부망에 개인정보를 저장하는 경우 위험도 분석 또는 영향평가 후에 암호화 적용범위 및 적용범위를 정하여 시행할 수 있습니다.

개인정보 저장시 암호화를 적용하는 경우 이 개인정보의 안전성 확보조치 기준 시행일로부터 3개월 이내에 암호화 계획을 수립하고, '12년 12월 31일까지 암호화를 적용하여야 합니다.



Q9

전산실 또는 자료보관실이 없는 중소기업입니다. “개인정보의 안전성 확보조치 기준” 제10조(물리적 접근방지) 조항을 준수해야 하나요?

기업의 규모에 상관없이 전산실, 자료보관실을 별도로 운영하고 있지 않으면 제10조(물리적 접근방지)는 적용되지 않습니다.

Q10

개인정보보호법 시행 이후 개인정보 안전성 확보조치(암호화 등), 주민등록번호 대체수단, 영향평가 등은 유예기간이 언제까지 인가요?

1. 암호화 등 개인정보의 안전성 확보조치 : 2012. 12. 31일 까지 완료(시행령 부칙 제4조)
2. 주민등록번호 외의 회원가입 방법 제공 의무 : 2012. 3. 30일부터 시행(시행령 부칙 제5조)
3. 개인정보영향평가 : 2012. 9. 30일까지 완료(개인정보영향평가에 관한 고시 및 해설서 제2조)

Q11

개인정보를 암호화해야 하는데 어떤 정보를 어디까지 암호화해야 하나요?

개인정보보호법 시행령 및 고시는 암호화 대상 개인정보로서 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호) 및 비밀번호, 바이오정보를 규정하고 있습니다.

개인정보를 정보통신망을 통해 전송하는 경우에는 위의 개인정보를 암호화하여 전송 및 저장하여야 합니다. 특히 비밀번호는 일방향 암호화하여 저장해야 합니다.

다만, 내부망에 고유식별정보를 저장하는 경우에는 자체 위험도 분석결과에 따라 암호화 적용여부 및 적용범위를 정할 수 있습니다.



Q12

개인정보 DB가 내부에 관리되면 암호화조치를 반드시 해야 하나요?

개인정보의 안전성 확보조치 기준 제7조 제5항에 따라 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있습니다.

1. 개인정보보호법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보영향평가의 결과
2. 위험도 분석에 따른 결과

Q13

고유식별정보인 여권번호(9자리) 중 일부(3~4자리)를 유일한 키를 생성하기 위해 사용할 경우에도 DB암호화가 필수사항인지요?

행정안전부의 개인정보의 안전성 확보조치 기준 제7조에 따르면, 고유식별정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우 또는 인터넷 구간 및 인터넷 구간과 내부망의 중간지점에 고유식별정보를 저장하는 경우에는 이를 암호화해야 하는 것을 원칙으로 하고 있습니다.

다만 내부망에 고유식별정보를 저장하는 경우에는 ①법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과와 ②위험도 분석에 따른 결과에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있습니다.

그러므로 여권번호 9자리 중 일부를 사용하는 것이 위 송·수신, 전달 또는 저장 중 어디에 해당하는지, 저장하는 경우에도 어느 곳에 저장되는지 여부에 따라 암호화 적용여부 및 적용범위가 달라질 수 있을 것으로 보입니다.



Q14

비밀번호에 대해 필수로 8자리를 하는 것이 맞나요?

개인정보의 안전성 확보조치 기준 및 해설서 제5조(비밀번호 관리) 규정에 의하면 개인 정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하도록 하고 있습니다.

즉, 안전하지 못한 비밀번호를 사용할 경우 정보가 노출될 위험성이 있으므로, 생일, 전화번호 등 추측하기 쉬운 숫자나 문자 등을 비밀번호로 이용하지 않도록 비밀번호 작성 규칙을 수립하고 개인정보처리시스템에 적용하여야 합니다.

이 때 비밀번호의 최소 길이는 구성하는 문자의 종류에 따라 최소 10자리 또는 8자리 이상의 길이로 구성하여야 하며, 이는 정보주체에 대한 비밀번호 작성규칙과는 달리 반드시 준수하여야 합니다. 참고로 비밀번호 작성규칙은 아래와 같습니다.

- 최소 10자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개) 중 2종류 이상으로 구성한 경우
- 최소 8자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9개, 10개) 및 특수문자(32개) 중 3종류 이상으로 구성한 경우

Q15

내부관리계획을 세워야 한다고 나와 있는데 내부관리계획과 지침은 같은 것으로 보는지, 지침이 있다면 계획은 수립하지 않아도 되나요?

내부관리계획의 수립은 개인정보의 안전성 확보에 필요한 기술적·관리적 및 물리적 조치 중의 하나입니다(법 제29조). 즉, 개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정절차를 통하여 수립·시행하는 내부 기준을 의미합니다. 따라서 내부관리계획을 기초로 세부 지침이나 안내서 등을 마련하여 개인정보 취급자 전원이 개인정보 보호에 필요한 동일한 기준에 따라 동일한 행동을 취하도록 할 필요가 있으므로, 내부관리계획은 반드시 수립·시행하여야 하며, 지침과는 별개의 것으로 판단됩니다.



나. 개인정보 처리방침의 수립 및 공개

Q1

각각의 사이트들마다 각각 “개인정보 처리방침”을 고지하여야 하나요?

웹사이트별로 운영목적 등이 다양할 수 있기 때문에 각 사이트의 특성을 고려하여 수집 정보나 수집목적이 다른 경우에는 개별적으로 고지하여야 할 것입니다.

만약, 수집하는 개인정보나 수집목적 등이 동일하다면 하나의 개인정보 처리방침을 수립하여 공동으로 사용할 수 있을 것입니다.

Q2

오프라인에서 회원가입 후 온라인상에서 주민등록번호와 이름을 입력하여 회원가입 유무를 확인하는데 개인정보 취급 또는 처리방침을 세워야 하나요?

온라인과 오프라인을 막론하고 개인정보를 처리하는 경우에는 원칙적으로 ‘개인정보 처리방침’을 정하여 공개해야 합니다(법 제30조).

개인정보 처리방침을 공개할 때에는 개인정보의 수집 장소와 매체 등을 고려하여 다음 중 하나 이상의 방법으로 공개하여야 합니다.

- ① 인터넷 홈페이지의 첫 화면 또는 첫 화면과의 연결화면을 통하여 이용자가 볼 수 있도록 하는 방법(글자 크기, 색상 등을 활용하여 개인정보 처리방침을 쉽게 확인할 수 있도록 표시해야 함)
- ② 점포 · 사무소 안의 보기 쉬운 장소에 써 붙이거나 비치하여 열람하도록 하는 방법
- ③ 같은 제목으로 연 2회 이상 계속적으로 발행하여 이용자에게 배포하는 간행물 · 소식지 · 홍보지 · 청구서 등에 지속적으로 게재하는 방법
- ④ 재화 또는 용역을 제공하기 위한 계약서에 게재하여 배포하는 방법



Q3

개인정보보호법상 ‘개인정보 처리방침’, 정보통신망 이용 촉진 및 정보보호 등에 관한 법률상 ‘개인정보 취급방침’ 중 어느 것을 사용해야 하나요?

정보통신망 이용촉진 및 정보보호 등에 관한 법률의 적용 대상인 정보통신서비스제공자는 개인정보 취급방침을 사용해야 하고, 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 적용 대상자가 아니라면 개인정보보호법에 따른 개인정보 처리방침을 사용하면 됩니다.

Q4

사업자인데요, 개인정보보호법 시행으로 개인정보취급방침을 어떻게 바꿔야 하나요?

정보통신망 이용촉진 및 정보보호 등에 관한 법률에 따른 정보통신서비스제공자라면 기존의 개인정보취급방침을 사용해도 무방할 것으로 보입니다.

정보통신서비스제공자가 아닌 경우에는 개인정보보호법 제30조 및 시행령 제31조에 따라 개인정보 처리방침을 작성하면 됩니다. 표준 개인정보보호 지침에 따르면 다음의 사항을 모두 포함하여야 합니다.

- ① 개인정보의 처리 목적
- ② 개인정보의 처리 및 보유 기간
- ③ 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
- ④ 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
- ⑤ 정보주체의 권리·의무 및 그 행사방법에 관한 사항
- ⑥ 처리하는 개인정보의 항목
- ⑦ 개인정보의 파기에 관한 사항
- ⑧ 개인정보 보호책임자에 관한 사항
- ⑨ 개인정보 처리방침의 변경에 관한 사항
- ⑩ 시행령 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항



다. 개인정보 보호책임자의 지정

Q1

자원봉사자의 정보를 저장하는 통합관리 사이트를 운영하는 경우에도 개인정보 보호책임자를 반드시 두어야 하고 파일도 출력물로 관리를 해야 하나요?

개인정보를 취급하고 있다면 개인정보 보호책임자를 지정해야 합니다. 개인정보 파일을 출력물로 관리를 하기 위해서는 법에 따른 보호조치를 취해야 합니다.

Q2

소규모 개인사업자도 개인정보 보호책임자를 지정해야 하나요?

개인정보보호법은 기업, 공공기관 등 모든 개인정보처리자에 대해 개인정보 보호책임자를 지정하도록 하고 있습니다. 공공기관 외의 개인정보처리자는 사업주 또는 대표자, 개인정보 관련 업무를 담당하는 부서의 장, 개인정보 보호에 관한 소양이 있는 사람 중에서 개인정보 보호책임자를 지정하도록 하고 있습니다. 따라서, 소규모 개인사업자의 경우에는 사업주나 대표자를 개인정보 보호책임자로 지정하면 됩니다.

라. 개인정보파일의 등록 및 공개

Q1

개인정보파일의 등록 및 공개는 무엇인가요?

공공기관이 개인정보파일 보유·운영 시 처리의 투명성 및 관리의 적정성을 위하여 개인정보파일 등록제를 실시하고 있습니다. 따라서 공공기관은 개인정보파일 운영시 명칭·운영근거·처리방법·보유기간 등을 등록해야 합니다.



◎ 개인정보파일 등록사항

- 개인정보파일의 명칭, 운영 근거 및 목적
- 개인정보파일에 기록되는 개인정보의 항목
- 개인정보의 처리방법 및 보유기간
- 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자

행정안전부 장관은 개인정보파일 등록시스템 구축·운영, 파일 등록현황 공개, 등록사항과 내용에 대한 개선권고 등을 시행합니다.

Q2

직원들의 PC내 보유중인 업무관련자 연락처도 행정안전부장관에게 등록 및 공개 해야하는 대상이 되는지요?

업무관련자 연락처는 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일에 해당될 수 있을 것으로 생각됩니다. 이 경우라면 개인정보보호법 제32조 제2항 제4호에 따라 등록대상에서 제외될 수 있습니다.

마. 개인정보 영향평가

Q1

공공기관은 영향평가를 무조건 해야 하나요?

영향평가의 대상기관은 개인정보보호법 시행령 제35조(개인정보보호법 제33조 제1항에서 위임)에 해당하는 개인정보파일을 구축·운영, 변경 또는 연계하려는 공공기관입니다. 영 제35조에 해당하는 개인정보파일은 다음과 같습니다.

1. 구축·운영 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운영하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운영하



고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일

3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일

Q2

2011년 3월부터 IT시스템 재구축을 시작하여 2012년 12월 31일까지 진행되는 프로젝트로 해당 프로젝트는 설계까지 마무리 되었고, 현재 개발을 진행 중에 있습니다. 이 경우 기존시스템으로 인정되어 5년 내에 영향평가를 받아도 되나요?

개인정보보호법 시행령 부칙 제6조에 따르면, 영 시행 당시 제35조 각 호에 따른 개인정보파일을 운용하고 있거나, 운용할 목적으로 제35조 각 호에 따른 개인정보파일을 구축하고 있는 공공기관의 장은 이 영 시행일로부터 5년 이내에 해당 개인정보파일에 대한 영향평가를 실시하고 그 결과를 행정안전부장관에게 제출하여야 한다고 규정하고 있습니다.

따라서 개인정보보호법 시행령 시행 당시(2011. 9. 30) 구축 중에 있으므로 영 시행일로부터 5년 이내에 영향평가를 수행하면 됩니다.

바. 개인정보 유출통지

Q1

개인정보 유출 통지는 어떤 방법으로 하나요?

개인정보처리자는 개인정보 유출시 지체 없이(5일 이내) 정보주체에게 유출사실을 통지해야 합니다. 또한, 1만명 이상 개인정보 유출시 지체 없이(5일 이내) 행정안전부 또는 한국인터넷진흥원, 한국정보화진흥원에 신고해야 합니다.

유출통지는 서면, 전자우편, FAX, 전화, 문자전송 또는 이에 상당하는 방법을 이용할



수 있습니다. 또한, 1만명 이상 개인정보 유출시에는 통지와 동시에 인터넷 홈페이지에 7일 이상 게재해야 합니다.

유출된 개인정보 확산 및 추가유출 방지를 위하여 접속경로 차단, 취약점 점검·보완, 유출 개인정보 삭제 등 긴급한 조치 필요시 해당 조치를 취한 후 정보주체에게 통지 가능합니다.

Q2

홈페이지 자체 점검시 게시자의 부주의로 인하여 개인정보가 홈페이지에 게재되어 있는 것을 알게 되었다면 유출사고가 아니더라도 정보주체에게 통지해야 하나요?

개인정보의 유출이라 함은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것으로서, 다음 각 호의 어느 하나에 해당하는 경우를 말합니다.

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우
4. 기타 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우

게시자의 부주의로 홈페이지에 개인정보가 노출된 것은 개인정보 유출에 해당하지 않습니다. 따라서 개인정보보호법 제34조에 따른 유출 통지 의무는 없습니다.

다만, 게시자의 부주의로 인하여 개인정보가 노출되어 있는 상황이라면 게시자에게 연락을 하여 해당 게시물에 대한 적절한 조치를 취하도록 해야 할 것입니다.



제 5 장

개인정보단체소송

Q1

단체소송은 무엇인가요?

단체소송은 다수의 정보주체가 피해를 입거나 피해를 입을 가능성이 높은 경우에 정보주체 각자가 침해에서 구제받거나 침해를 예방하기 위해 소송을 제기하는 것은 거의 불가능하므로 일정한 자격을 갖춘 단체가 당사자적격을 부여받아 정보주체에 대한 침해행위에 대처할 수 있도록 하기 위해 도입되었습니다.

따라서, 개인정보보호법 제51조 각 호의 규정에 해당하는 단체는 개인정보처리자가 제49조에 따른 집단분쟁조정을 거부하거나 집단분쟁조정의 결과를 수락하지 아니한 경우, 법원에 권리침해 행위의 금지·중지를 구하는 소송을 제기할 수 있습니다.

Q2

개인도 단체소송을 제기할 수 있나요?

개인정보 단체소송을 제기할 수 있는 단체는 소비자단체와 비영리민간단체로 제한되므로 개인은 단체소송을 제기할 수 없습니다.

개인정보 단체소송을 제기할 수 있는 소비자단체는, ①「소비자기본법」 제29조의 규정에 따라 공정거래위원회에 등록된 소비자단체로서, ②정관에 따라 상시적으로 정보주체의 권익증진을 단체의 주된 목적으로 하며, ③단체의 정회원수가 1천명 이상이고, ④공정거래위원회에 등록 후 3년이 경과했어야 합니다.

개인정보 단체소송을 제기할 수 있는 비영리민간단체는, ①비영리민간단체 지원법 제



2조의 규정에 따른 비영리민간단체로서, ②법률상 또는 사실상 동일한 침해를 입은 100인 이상의 정보주체로부터 단체소송의 제기를 요청받아야 하고, ③정관에 개인정보 보호를 단체의 목적으로 명시한 후 최근 3년 이상 이를 위한 활동실적이 있어야 하며, ④단체의 상시 구성원수가 5천명 이상이며, ⑤중앙행정기관에 등록되어 있어야 합니다.

Q3

단체소송의 대상과 청구범위는 어떻게 되나요?

개인정보단체소송의 대상이 되는 개인정보처리자의 행위는 개인정보처리와 관련한 정보주체의 권리를 침해하는 행위입니다. 반드시 개인정보보호법 위반에 따른 권리침해 행위에 한정하지 않고 개인정보처리와 관련해서 발생한 권리침해행위는 모두 단체소송의 대상이 됩니다. 소재지 당시 권리침해 행위가 계속되고 있어야 하고 과거의 권리침해행위는 단체소송의 대상이 되지 못합니다.

개인정보단체소송의 청구범위는 권리침해행위의 금지·중지 청구만을 그 내용으로 하기 때문에 개인정보 유출 또는 오남용으로 인한 손해배상을 청구할 수는 없으며, 정보주체가 손해배상을 청구하기 위해서는 개별적으로 소송을 제기해야 합니다.

Q4

단체소송에서 전속관할이 무엇인가요?

개인정보 단체소송의 소는 피고의 주된 사무소 또는 영업소가 있는 곳의 지방법원 본원 합의부의 관할에 전속합니다. 그러나 주된 사무소나 영업소가 없는 경우에는 주된 업무담당자의 주소가 있는 곳의 지방법원 본원 합의부의 관할에 전속합니다.

피고가 외국사업자인 경우에는 대한민국에 있는 이들의 주된 사무소·영업소 또는 업무담당자의 주소에 따라 정합니다.



개인정보보호법 상담사례집



행정안전부

KISA 한국인터넷진흥원
Korea Internet & Security Agency