KOTRA자료 22-086

우리 기업이 꼭 알아야 할 중국 개인정보보호법 가이드북

kotra
Korea Trade-Investment Promotion Agency

목 차

본 가이드북은 우리 기업들의 중국 개인정보보호법 준수를 위해 법의 주요 정, 준법구조, 업무 유형별 개인정보보호 대응 시나리오 등을 정리하여 참고용으로 제공하는 것입니다. 따라서, 내용의 일부 또는 전체로 인하여 발생 가능한 모든 결과에 대하여 일체의 책임이 없음을 밝힙니다.

본 가이드북은 중국 로펌인 중룬법률사무소(中伦律师事务所)에서 중국어 원문을 제공하였고, 법무법인태평양 상해사무소에서 한글 번역본 감수를 받았습니다.

제 1장 개요

「중화인민공화국 개인정보 보호법」(이하 "「개인정보 보호법」")은 2021년 11월 1일부터 정식으로 시행되었으며, 총 8장 74조로 구성되어 있다.
「개인정보 보호법」이란 용어를 들었을 때 무엇이 가장 먼저 떠오르는가? 아마도 자신의 개인정보가 이 법에 의해 보호될 수 있을 것이라는 생각이 들 수 있을 것이다. 기업[1]의 입장에서는 이 법에 따라 고객은 물론 직원 및 거래처 담당자의 개인정보까지 보호해야 할 의무가 발생하고, 내부적으로 어떻게 개인정보보호 대책을 마련하고 개선해야 할지 고민이 될 것이다. 이 자료는 기업의 입장에서 꼭 알아야 할 중국의 「개인정보 보호법」 내용에 대해 다루고 있다.

기업 입장에서 「개인정보 보호법」의 어떤 내용을 알아 두어야 할까?

첫째, 개인정보의 범위와 종류를 알아야 한다. 어떤 정보가 개인정보에 해당하는지에 대해 명확히 알아야 한다. 또한, 개인정보 중 더욱 주의하여 보호하여야 하는 '민감 개인정보', '아동 개인정보'가 무엇인지에 대해서도 알아야 한다. 따라서, 다양한 개인정보에 대해 법규정에 따라 종류별로 그 범위 및 등급을 분류하여 각 개인정보에 요구되는 의무를 준수할 수 있는 준법감시(compliance) 시스템을 갖추어야 한다.

둘째, 개인정보보호 원칙을 알아야 한다. 「개인정보 보호법」 제1장은 개인정보 보호에 관한 5대 원칙을 명확히 규정하고 있다. 기업은 이 5대 원칙을 숙지해야 하며 개인정보보호 준법감시(compliance) 시스템을 구축하거나 개인정보를 처리할 때 이러한 원칙을 준수해야 한다. 아울러, 이러한 원칙에 위배되는 행위가 발생할 경우, 제때에 이를 시정하여 불이익을 받지 않도록 예방해야 한다.

셋째, 개인정보 주체의 권리행사에 대한 의미를 명확하게 파악해야 한다. 「개인정보 보호법」 제4장에선 개인정보 주체[2]의 권리를 규정하고 있다. 이러한 권리는 네트워크 안전과 데이터 보호에 관한 기타 법률이나 법규뿐만 아니라, 「민법전」[3]

1) 「개인정보 보호법」은 기업뿐 아니라 개인도 준수해야 하지만 편의상 본 가이드북에서는 기업 입장에서 유의할 점을 주로 서술하였다.
2) 한국 개인정보 보호법은 "정보주체"라고 정의한다(한국 개인정보 보호법 제2조 제3호)
3) 한국의 민법에 상응하는 법률은 중국에서 "민법전"(民法典)이라고 한다.

및 「소비자권익보호법」과도 연계되어 있다. 따라서, 개인이 권리를 행사할 때 기업은 관련 요청사항에 정확하고 신속하게 대응하기 위해 개인정보 처리 과정에 있어 개인의 권리를 명확하게 파악하고 적절한 대응 시스템을 구축해야 한다.

넷째, 개인정보 처리에 관한 규칙을 정비해야 한다. 「개인정보 보호법」 제2장 및 제3장에선 다양한 경우에 따른 개인정보 처리 방법과 규칙을 규정하고 있다. 이러한 규칙에는 중화인민공화국(이하 "중국") 내에서 개인정보를 처리하기 위한 요구 사항과 규범뿐만 아니라 개인정보의 국외 이전에 대한 요구 사항 및 규범도 포함되어 있다. 따라서 기업은 중국 국내외의 데이터 처리 전 과정을 살펴보고 법규정에 부합되지 않는 부분에 대해서는 모두 시정할 필요가 있다.

다섯째, 개인정보처리자의 의무를 숙지해야 한다. 기업은 개인정보 처리에 관한 규칙 외에 개인정보보호 의무에 대해서도 주의를 기울여야 하며, 이러한 의무는 「개인정보 보호법」 제5장에 명시되어 있다. 따라서 기업은 개인정보처리자의 의무에 관한 규정을 정비하여 이행해야 한다.

여섯째, 관련 행정부서의 감독 및 심사에 협조해야 한다. 기업은 「개인정보 보호법」에서 규정하고 있는 중국의 관할 행정부서를 파악하고 법령에 따라 해당 행정부서의 감독 및 심사 업무에 협조해야 한다.

중국은 이미 플랫폼 경제시대, 정보화 시대, 4차 산업혁명의 시대에 들어섰다. 빅데이터와 인공지능이 광범위하게 활용되는 4차 산업혁명의 시대에서 개인정보는 미래산업의 원유(原油)와도 같은 역할을 할 것으로 기대된다. 기업들은 중국 「개인정보 보호법」에 위배되지 않도록 준법감시(compliance) 제도를 정비해야 할 필요가 있다. 조금 더 적극적인 기업이라면 개인정보의 적합한 활용을 통해 4차 산업 시대 새로운 비즈니스 경쟁력을 확보 할 수도 있을 것이다.

제 2장 「개인정보 보호법」 주요 정의

기업들은 「개인정보 보호법」 의 아래 정의에 대해 주의를 기울일 필요가 있다.

제 1절 개인정보

개인정보의 정의: 「개인정보 보호법」 제4조에 따르면, “개인정보”란 전자 또는 기타 방식으로 기록되어 식별되었거나 식별이 가능한 자연인과 관련된 각종 정보를 의미하며, 익명화 처리된 후의 정보는 제외된다.

예시: 자연인의 성명, 생일, 유효한 증명서 번호, 혼인상태, 직장, 학력, 경력, 자택주소, 전화번호 등 기록되어 식별되었거나 식별이 가능한 자연인과 관련된 정보는 모두 개인정보 범위에 해당될 수 있다.

유의 사항

개인정보의 범위는 자연인 개인의 정보에 한하며, 기업이나 재단 등 기타 법인이나 기관의 정보는 개인정보에 해당하지 아니한다.

익명화 처리된 정보는 개인정보에 해당하지 아니한다. 즉 특정 자연인의 개인정보가 익명화 처리된 이후에는 개인정보로 간주되지 않는다. “익명화 처리”의 의미에 대해서는 뒷부분에서 설명하도록 한다.

※ 한국법상 “개인정보”의 개념

[한국 개인정보 보호법 제2조 제1호]

“개인정보”는 살아있는 개인에 관한 정보로서 다음 어느 하나에 해당하는 정보

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 가명 처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보

※ 한국법상 “고유식별정보”의 개념

[한국 개인정보 보호법 시행령 제19조]
1. 「주민등록법」 제7조 제1항에 따른 주민등록번호
2. 「여권법」 제7조 제1항 제1호에 따른 여권번호
3. 「도로교통법」 제80조에 따른 운전면허의 면허번호
4. 「출입국관리법」 제31조 제5항에 따른 외국인등록번호

(참고: 한국 개인정보 보호법에는 위 4가지를 “고유식별정보”로 정의하고 개인정보처리자의 고유식별정보 처리를 엄격히 제한하고 있으나 중국법에는 고유식별정보 개념은 없음)

제 2절 민감 개인정보

민감 개인정보의 정의: 「개인정보 보호법」 제28조에 따르면, “민감 개인정보”란 일단 유출되거나 불법으로 사용될 경우 자연인의 인격 존엄성이 쉽게 침해될 수 있거나 신체적 또는 금전적 안전에 쉽게 위험을 초래할 수 있는 개인정보로서 생체인식, 종교신앙, 특정 신분, 의료건강, 금융계좌, 위치 및 행적 등 정보와 만 14세 미만 미성년자의 개인정보가 포함된다.[4)]

<u>예시</u>: 민감 개인정보는 매우 다양한 바 개인의 재산정보(은행계좌, 예금정보, 신용정보 등), 건강 및 생리 정보(진료지시서, 검사보고서, 과거 병력 등), 생체인식정보(유전자, 지문, 안면인식 특징 등), 신원정보(신분증, 운전면허증, 거주허가증 등)는 물론 성적 취향, 종교신앙, 통신 기록 및 내용, 주소록, 친구 목록, 웹 검색 기록 등 자연인이 일반적으로 다른 사람에게 공개하지 않는 정보를 포함한다.

<u>유의 사항</u>

민감 개인정보의 판단 기준: 특정 개인정보가 민감 개인정보인지 여부를 판단할 때에는 해당 개인정보가 유출되거나 불법적으로 제공 또는 남용되었을 때 자연인의 신체적•금전적 안전에 위험을 초래할 수 있는지 여부와 개인의 명예, 심신 건강에 대한 손해나 차별적 대우를 쉽게 받을 수 있는지 여부에 중점을 두어야 한다. 만약 상기 불이익이 발생하거나 발생할 가능성이 존재하는 경우, 해당 정보를

4) 중국 «정보안전기술 개인정보안전규범»(GB/T 35273-2020)(이하 “개인정보안전규범”)은 민감 개인정보를 예시하고 있다. 개인정보안전규범은 법적 효력은 없으나 중국 정부가 법 집행을 함에 있어 가이드라인의 역할을 한다.

민감 개인정보로 간주해야 한다. 예를 들어, 자연인의 신분증 사본을 제3 자의 휴대전화 카드 실명등록, 은행계좌 및 신용카드 개설 등에 사용하거나, 또는 개인정보 주체의 동의 없이 건강정보를 보험회사의 마케팅이나 개인 보험료 산정에 사용할 경우, 개별 주체의 권익에 중대한 위험을 초래할 수 있으므로 민감 개인정보로 간주해야 한다.

만 14세 미만 미성년자의 모든 개인정보는 민감 개인정보에 해당한다. 따라서, 기업은 정보 수집 시 미성년자 정보를 포함하는지 여부에 주의를 기울여야 하고, 그 중 만 14세 미만 미성년자에 관한 개인정보 처리사항들을 면밀히 살펴보아야 한다.

※ 한국법상 "민감정보"의 개념

[한국 개인정보 보호법 제23조 및 개인정보 보호법 시행령 제18조]
사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조 제2항 제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.

1. 유전자검사 등의 결과로 얻어진 유전정보
2. 「형의 실효 등에 관한 법률」 제2조 제5호에 따른 범죄경력자료에 해당하는 정보
3. 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보
4. 인종이나 민족에 관한 정보

제 3절 개인정보의 처리

개인정보 처리의 정의: 「개인정보 보호법」 제4조에 따르면, "개인정보의 처리"는 개인정보의 수집•보관•이용•가공•전송•제공•공개•삭제 등을 포함한다. 다시 말해, "처리"라는 표현은 앞서 언급한 모든 행위를 포함하여 개인정보에 대해 취해지는 행위에 대한 포괄적인 개념이다.

예시: 개인정보 처리의 정의는 개인정보를 처리하는 관련 주체의 모든 행위를

포함하므로 기업이 개인정보의 수집•보관•이용•가공•전송•제공•공개•삭제 등의 행위를 하는 경우에는 「개인정보 보호법」을 준수해야 한다. 예를 들어, 특정 기업이 고객의 취향에 보다 적합한 제품(상품)을 생산하기 위해 고객 데이터를 수집하여 선호도를 분석하는 행위에 있어, 개인정보를 수집 및 이용하는 행위가 곧 개인정보의 처리에 해당한다.

유의 사항: 개인정보의 처리는 개인정보 생애주기 전체 과정을 포괄하는 개념이므로, 기업은 개인정보 처리활동 및 범위를 명확히 하고 각 처리 단계별 법령상 요구사항을 파악한 후, 이를 토대로 준법감시(compliance) 시스템을 구축하여 법령에 부합하도록 해야 한다.

제 4절 개인정보처리자

개인정보처리자의 정의: 「개인정보 보호법」 제73조에 따르면, "개인정보처리자"란 자율적으로 처리목적, 처리방법 등 개인정보 처리사항을 결정하는 기관 또는 개인을 의미한다.

예시: 예를 들어 중국 경내에서 개인정보를 처리하는 우리 나라 기업의 중국지사(자회사, 사무소 등) 또는 해당 중국 지사로부터 개인정보를 제공받아서 처리하는 한국 본사 모두 개인정보처리자에 해당하며 「개인정보 보호법」을 준수해야 한다.

유의 사항

개인정보처리자는 다양한 기관 또는 개인을 포함하므로 기업, 비법인단체, 자연인 모두가 개인정보처리자가 될 수 있다.

기업은 「개인정보 보호법」에 따른 "개인정보처리자"의 정의가 '유럽 일반 개인정보보호규정(General Data Protection Regulation, 이하 "GDPR")' 상의 "정보처리자(processor)"와는 다르고 "정보제어자(controller)"와 유사하다는 점에 유의해야 한다.

제 5절 자동화 의사결정(알고리즘의 차별 선택)

자동화 의사결정의 정의: 「개인정보 보호법」 제73조에 따르면, “자동화 의사결정”이란 컴퓨터 프로그램을 이용하여 개인의 행위 및 습관, 취미 및 취향 또는 경제, 건강, 신용 등 정보를 자동으로 분석•평가하고 의사를 결정하는 행위를 의미한다.

예시: 자동화 의사결정은 이미 우리 삶의 곳곳에 깊숙이 자리잡고 있다. 우리가 매일 접하는 정보, 쇼트 클립, 광고 및 인공지능기반 주식 투자나 건강 어드바이저 등은 모두 자동화 의사결정과 밀접한 연관이 있다. 예를 들어, 개인이 온라인으로 대출을 신청하는 경우 신청자의 신용점수에 따라 자동으로 승인 또는 거절되는데, 이러한 의사결정 방식이 곧 자동화 의사결정에 속한다. 또 예를 들어 차량의 속도, 방향, 차선 및 신호등 상태, 교통표지판을 기반으로 법규 위반 여부를 자동으로 판단하는 것도 자동화 의사결정에 해당한다.

유의 사항: 2019년 1월 1일부터 시행된 중국의 <전자상거래법> 에서는 인터넷 플랫폼이 동일한 제품 및 서비스에 대해 기존고객에게 신규 고객보다 더 높은 가격을 제시하는 소비자 차별대우 행위(이른바 大数据杀熟)를 규제하고 있다. 동법 제 18조에서는 소비자의 취미, 소비 습관 등 특징에 따라 제품 및 서비스에 관한 검색결과를 제공함과 동시에 그 소비자에게 특화(맞춤형)되지 않은 옵션 또한 제공해야 한다고 규정하고 있다. 「개인정보 보호법」은 이러한 규정의 입법취지를 반영하여, 자동화 의사결정에 대해 보다 엄격한 처리 규정을 제시하고 있기 때문에, 기업은 제품개발 및 디자인 단계에 자동화 의사결정 관련 법령을 반영하는 동시에, 자동화 의사결정 및 알고리즘 규제 분야에 있어 중국의 입법 동향을 주시할 필요가 있다.

제 6절 비식별화

비식별화 정의: 「개인정보 보호법」 제73조에 따르면, “비식별화”란 개인정보를 처리하여 추가 정보의 도움 없이는 특정 자연인을 식별할 수 없도록 하는 과정을

의미한다. 개인정보 비식별화의 목적은 개별 정보의 특정 개인에 대한 식별 정도를 낮춤으로써 해당 작업을 거친 특정 개인정보를 통해 특정 개인을 식별하기 어렵게 하는데 있다.

예시: 성명을 예로 들면, 흔히 볼 수 있는 비식별화 방법은 다음과 같다.
포괄적이고 추상적인 기호로 표시함. 예컨대, "Mr./Miss Kim" 등.
성명을 삭제하거나 또는 통일된 기호인 "*" [5] 등으로 표시함.
랜덤으로 생성된 한자 등으로 성명을 표시함. 예컨대, "일이(一二)"로 "장웨이(张伟)"를 표시함.

유의 사항

비식별화 처리 후의 정보일지라도 개인정보를 바탕으로 생성되었기 때문에 개인정보의 세분성(granularity)을 지니고 있으므로 여전히 개인정보에 해당한다. 따라서 기업은 개인정보에 대해 비식별화 처리하였더라도 여전히 개인정보보호 규정을 준수해야 한다.
비식별화는 개인정보 처리에 따른 위험 부담을 줄이고 유출로 인한 피해를 통제하는 것에 효과적으로 도움되므로, 기업은 비식별화 기술의 적용에 관심을 기울어야 한다.

※ 중국법상 "비식별화"와 유사한 한국법상 "가명처리"의 개념

[한국 개인정보 보호법 제2조 제1의2호]
"가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

제 7절 익명화 처리

익명화 처리의 정의: 「개인정보 보호법」 제73조에 따르면, "익명화 처리"란 개인정보를 처리하여 특정 자연인을 식별하지 못하게 하며 다시 복원시키지

5) 다른 추가 정보가 삭제된 상태에서 'Ms/Mr. Kim' 또는 '*' 등으로 표기 후 복원할 수 없도록 처리한 경우에는 익명화 처리가 되었다고 볼 수 있다. 비식별화는 다른 추가 정보와 함께 보면 특정 자연인을 식별할 수 없도록 하는 것을 의미한다. 반대로 해석하면, 다른 추가 정보의 도움으로 특정 자연인을 식별하는 것이 가능한 경우에는 비식별화된 개인정보에 해당할 수 없다.

못하도록 만드는 과정을 의미한다. 「개인정보 보호법」 제4조에 따르면 익명화 처리 된 정보는 개인정보에 해당하지 아니한다.

예시: 데이터의 무작위처리와 데이터 일반화가 일반적인 익명화 처리 기술이다. 데이터 무작위처리는 데이터의 정확성을 줄여 데이터와 개인 간의 연계를 모호하게 하는 것을 말하고, 데이터 일반화는 낮은 수준의 개념(예: 특정 나이)을 높은 수준의 개념(예: 청년, 중년, 노인)으로 대체하는 것을 말한다.

유의 사항

기업이 어떤 종류의 익명화 처리 기술을 채택하는지를 불문하고 반드시 다음과 같은 효과를 달성해야 한다. (1) 익명화 처리된 정보만으로 특정 개인을 식별할 수 없어야 함. (2) 익명화 처리된 정보가 기타 정보와 결합되더라도 특정 개인을 식별할 수 없어야 함. (3) 익명화 처리된 정보를 입수한 주체가 일반적으로 가능한 조치를 취하더라도 특정 개인을 식별할 수 없어야 함(즉, 복원 불가).
익명화 처리는 매우 높은 요구 사항이므로, 기업은 개인정보에 대해 관련 기술을 채택한 후 익명화 처리 규정을 충족할 수 있는지 여부를 신중하게 판단해야 한다.

※ 한국법상 "익명처리"의 개념

[한국 신용정보의 이용 및 보호에 관한 법률 제2조 제17호]
"익명처리"란 더 이상 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리하는 것을 말한다.
(참고: 한국 개인정보 보호법에는 "익명처리"라는 용어를 쓰고 있으나 정의 조항은 없음)

제 8절 정보의 국외 이전

국외 이전의 정의: 「개인정보 보호법」 제38조에 따르면, "국외 이전"이란 중국 내에서 수집된 개인정보를 중국 밖 국가나 지역으로 전송하는 것을 의미한다.

예시: 예를 들어 한국기업의 중국지사(예: 자회사, 계열사)가 중국에서 수집한

개인정보(예: 중국 직원의 개인정보)를 한국 본사에 제공하는 경우 국외 이전에 해당한다.

유의 사항

국외 이전 시 반드시 「개인정보 보호법」 규정을 준수해야 한다. 기업이 개인정보를 국외로 이전하는 경우, 반드시 국가네트워크정보 당국에서 주관하는 안전성 평가를 통과하거나, 또는 국가네트워크정보 당국이 인정하는 전문 기관으로부터 개인정보보호 인증을 취득하거나, 또는 중국정부가 제정한 표준 계약서에 국외 이전에 관한 사항을 표준 약정으로 명시해야 한다.

중국 국내에 있는 기업이 중국 국내의 개인정보를 중국 국외에 제공하는 경우, 개인정보를 이전 받는 중국 국외의 자가 개인정보를 어떻게 처리할 것인지를 불문하고, 반드시 「개인정보 보호법」에 따른 국외 이전 규칙을 준수해야 한다. 「개인정보 보호법」 제3조에 따르면, 국외에서 개인정보를 이전 받는 자가 중국 국내의 자연인을 대상으로 제품 또는 서비스를 제공하거나 중국 국내의 자연인을 분석 또는 평가할 목적으로 개인정보를 처리하는 경우, 마찬가지로 「개인정보 보호법」의 규정을 준수해야 한다.

중국의 법체계에 따라 중국 대륙과 홍콩•마카오•대만 간의 개인정보 전송도 국외 이전에 해당한다. 따라서 중국 대륙 지역에 위치한 기업이 홍콩•마카오•대만 지역에 위치한 자에게 중국 대륙 지역의 개인정보를 제공하는 행위도 국외 이전에 해당한다.

제 9절 서면 동의

서면 동의의 정의: “서면 동의”란 구두가 아닌 서면 문자 형식으로 동의를 표시하는 것을 의미한다. 「개인정보 보호법」 제14조와 제29조에 따르면, 중국의 법령상 특정 개인정보, 특히 민감 개인정보의 처리 상황에 해당하는 경우 개인정보 주체로부터 서면 동의를 취득하도록 규정하고 있다.

예시: 「신용조사업 관리조례」 제18조에 따르면, 법에 의해 달리 정해진 경우를 제외하고 기업이 신용정보기관으로부터 고객의 개인신용보고서 등 개인정보를

조회하고자 할 경우 해당 고객의 서면 동의를 얻어야 한다.

유의 사항: “서면”이라 함은 단순히 종이 형태를 말하는 것이 아니라 언제든지 열람하고 조회할 수 있는 가시적인 형태면 되므로, 흔히 이용자가 웹사이트나 애플리케이션에서 ‘동의’를 클릭하면 서면 동의의 요건을 충족할 수 있다.

제 10절 별도의 동의

별도 동의의 정의: “별도의 동의”란 일반적인 개인정보처리 동의와는 다른 별개의 동의를 말하며, 보다 높은 수준의 동의를 말한다. 개인정보를 처리하는 일부 행위는 개인정보 주체로부터 별도의 동의를 얻어야 한다.

예시: 중국에서 운영 중인 애플리케이션(App)의 경우, 이용자에게 보다 적합한 광고를 제공하기 위해 이용자의 개인정보를 광고업체에게 제공하는 경우 이용자로부터 별도의 동의를 얻어야 한다.

유의 사항: 「개인정보 보호법」에 따르면 (i) 민감 개인정보 처리(제29조), (ii) 다른 개인정보처리자에게 개인정보 제공(제23조), (iii) 개인정보 공개(제25조), (iv) 국외 이전(제39조), (v) 공공장소에서 수집된 개인 사진, 신원식별 정보 등을 공공의 안전이 아닌 다른 목적을 위해 사용하는 경우(제26조)에는 모두 개인의 별도 동의가 필요하며, 자세한 내용은 후술하도록 한다. 현재 실무상 법령에 명확한 요구가 있는 경우에만 “별도의 동의”가[6] 필요하다는 것이 업계 다수의 견해이다.

제 11절 핵심정보인프라시설 운영자

핵심정보인프라시설의 정의: 통신•에너지•교통•수자원•금융•공공서비스•전자정부 등 주요 산업 및 분야, 또는 파괴, 기능 상실 및 정보 유출로 인해 중국의 국가

6) 개인정보 처리의 적법성 근거 관련 내용은 본 가이드북 제3장 개인정보 준법 구조의 제3.4절 개인정보 처리 규칙 제1항 개인정보 처리의 기본 근거를 참조.

안보와 공공의 이익에 중대한 피해를 초래할 수 있는 주요 네트워크 시설이나 정보 시스템 등이 핵심정보인프라시설에 해당된다. 나아가 해당 시설 사업자가 곧 핵심정보인프라시설 운영자일 수 있다. 「개인정보 보호법」은 핵심정보인프라시설 운영자에 대해 더욱 엄격한 개인정보보호에 관한 의무를 부과하고 있으며, 자세한 내용은 후술하도록 한다.

유의 사항

「핵심정보인프라시설 보안 보호 조례」에 따라 중국의 각 산업별 감독기관은 산하 업계의 핵심정보인프라시설 운영자를 지정하고 해당 사업자에게 고지하는 업무를 담당하고 있다. 따라서 지금까지 중국 정부기관으로부터 핵심정보인프라시설 운영자로 지정되었다는 통보를 받지 못한 기업은 일단 핵심정보인프라시설 운영자가 아닌 것으로 볼 수 있다.

만약 핵심정보인프라시설 운영자로 지정될 경우 더욱 엄격한 안전보호조치가 요구된다. 예를 들어, 전문 보안관리 기구를 구성하여 정기적으로 네트워크안전 점검 및 위험 평가에 이어, 네트워크 제품 및 서비스 공급자와 '보안 비밀유지 계약'을 체결해야 한다.

기업이 영위하는 산업 또는 분야 및 그 규모가 앞서 언급한 주요 산업 또는 분야에 해당하지 않더라도 중국의 법령에 따라 기업의 협력사가 핵심정보인프라시설 운영자에 해당하는 경우, 해당 핵심정보 인프라시설 운영자는 기업을 상대로 다음과 같은 내용을 요구할 수 있다. (1) 중국 현지 보관 협력 프로젝트 중 취득한 개인정보와 중요한 데이터 파기 요청. (2) '보안 비밀유지 계약' 체결 요청. (3) 네트워크안전 심사 협조 요청. (4) 개인정보보호 영향평가 협조 요청 등. 따라서 기업은 핵심정보인프라시설 운영자와 협력하고자 할 때 자사의 여건과 사업타당성을 충분히 점검한 후, 「개인정보 보호법」을 위반하지 않도록 사업을 전개해야 한다.

제 3장 개인정보 준법 구조

제 1절 개인정보 보호법의 적용 범위

「개인정보 보호법」의 적용 범위 판단은 "속지주의 원칙" + "예외적 역외적용"을 기준으로 한다. 다시 말해, 「개인정보 보호법」의 적용 범위는 중국내의 개인정보 처리자는 물론 일부 국외의 개인정보 처리자도 포함한다.

속지주의 원칙: 「개인정보 보호법」 제3조 제1항은 법률 적용 범위의 기본 원칙인 속지주의 원칙을 규정하고 있다. 즉, 개인정보 처리활동의 발생지를 기준으로 삼는다는 의미로써 개인정보처리자가 중국 기업 혹은 외국계 기업을 불문하고, 개인정보 처리 주체가 중국 국민여부와 상관없이 개인정보 처리활동이 중국 내에서 발생하면 「개인정보 보호법」을 적용 받아야 한다.

예외적 역외적용: 「개인정보 보호법」 제3조 제2항은 법률 적용 범위의 보완 원칙인 지향주의 원칙(예외적 역외적용)을 규정하고 있다. 중국 국외에서 개인정보를 처리하는 주체일지라도 다음의 경우에 해당하는 경우 「개인정보 보호법」이 적용된다. (1) 국외의 개인정보 처리자가 처리하는 개인정보가 중국 국내 자연인의 정보이고, 영위하는 사업이 중국 국내 자연인에게 제품, 서비스를 제공하는 행위에 해당하는 경우. 예를 들어, 중국 소비자를 대상으로 하는 중국 국외에 위치한 전자상거래 플랫폼, 면세점, 화장품 회사, 의류회사 기타 소비재 회사 등이 중국 국내로 제품 또는 서비스를 제공하는 경우 「개인정보 보호법」 규정을 준수해야 한다. (2) 국외의 개인정보 처리자가 중국 국내 자연인의 개인정보를 이용하여 그 행위를 분석, 평가하는 경우. 예를 들어, 중국의 소비자를 대상으로 하는 온라인 게임사, 호텔이나 마케팅 분석기관이 중국 국내 소비자의 선호도를 분석, 처리하는 경우 「개인정보 보호법」 규정을 준수해야 한다.

유의 사항
중국 외에 소재 기업이 「개인정보 보호법」의 적용 대상에 해당하는지 여부를 결정하기 위해서는 판단 기준과 프로세스를 구축해야 한다. (1) 개인정보 처리활동의 발생지가 중국 국내에 위치한 것인지 여부를 명확히 해야 한다. (2) 개인정보 처리활동의 발생지가 국외인 경우, 제품 및 서비스를 제공받는 단체 또는 분석, 평가 대상 중에 중국 국내 자연인이 포함되는지 여부를 확인해야 한다. 만약 「개인정보 보호법」 제3조 규정에 해당하는 경우 「개인정보 보호법」 규정을 준수해야 한다.

제 2절 개인정보 보호법의 기본 원칙

「개인정보 보호법」 제5조 ~ 제9조에서는 개인정보 처리에 관한 5가지 기본 원칙, 즉 (i) 적법성, 정당성, 필요성, 신의성실의 원칙; (ii) 합리적 목적 및 최소 범위 원칙; (iii) 공개□투명 원칙; (iv) 정확성 원칙; (v) 책임성 및 데이터 보안 원칙을 규정하고 있다. 상기 5가지 기본 원칙은 「개인정보 보호법」의 입법취지를 반영하였는바, 일부 개인정보 처리활동에 대해 직접 적용 가능한 법령이나 구체적인 조항이 없는 경우 위와 같은 기본 원칙을 근간으로 개인정보를 처리할 것을 요구한다.

가. 적법, 정당, 필요, 신의성실의 원칙

「개인정보 보호법」 제5조에 따르면, 개인정보를 처리함에 있어 적법성, 정당성, 필요성 및 신의성실의 원칙을 준수해야 한다.

“적법성 원칙”이란 개인정보 처리활동은 반드시 중국의 법령을 준수해야 하는 것을 의미한다.

“정당성 원칙”이란 개인정보처리자가 개인정보 처리활동을 수행할 때 그 목적과 수단이 정당성을 갖추어야 하고, 공평과 정의의 이념에 부합해야 하며, 개인정보 처리활동이 개인정보 주체에게 피해를 초래하면 아니 됨을 의미한다.

“필요성 원칙”이란 개인정보 처리활동이 필요성을 갖추어야 하며, 개인정보에 대한 과도한, 무질서한, 혼란스러운 사용을 예방함으로써 개인정보주체의 권익을 보호함을 의미한다.

“신의성실의 원칙”이란 개인정보처리자 및 개인정보 처리활동이 신의에 따라 성실하게 이루어져야 하며 오도(誤導), 사기, 협박 등 방식으로 개인정보 주체가 하나 또는 다수의 개인정보 처리활동 요구사항을 수락하도록 강요하면 아니 됨을 의미한다.

유의 사항
2021년 3월 22일 국가네트워크정보 당국에서 「일반 유형의 모바일 인터넷 앱에 필요한 개인정보 범위에 관한 규정」을 공포하였는바, 중국 당국은 이미 필요 원칙을 개인정보 처리활동에 대한 준법 심사의 핵심으로 삼고 있다는 점을 알 수 있다. 따라서 개인정보 처리활동의 필요 원칙을 보장하기 위해 경영과정 중 개인정보 처리 체계와 행위에 대해 면밀히 점검해야 한다.

나. 합리적 목적 및 최소 범위 원칙

「개인정보 보호법」 제6조에 따르면, 개인정보처리자가 개인정보를 처리할 때 합리적 목적 및 최소 범위의 원칙을 준수해야 한다.

가. “합리적 목적” 원칙이란 개인정보 처리활동의 목적이 명확하고 분명하며 구체적이어야 하고, 개인정보 처리활동이 처리목적과 직접적 관련이 있어야 함을 의미한다.

나. “최소 범위” 원칙이란 개인정보의 수집은 처리목적을 위한 최소한의 범위로 제한되어야 하며, 개인정보를 과도하게 수집하면 아니 됨을 의미한다. 해당 원칙은 개인정보 처리활동의 최초 단계에서 개인정보의 수집을 제한함으로써, 개인정보 주체에 대한 보호를 원천적으로 강화하려는데 그 목적을 두고 있다. 예를 들어, 특정 서비스의 제공과 무관한 월 수입, 혼인 여부 등에 관한 정보는 최소 범위 수집 원칙에 위반된다고 볼 수 있다. 또한 기업이 자동 수집 툴을 이용하여 개인정보를 수집하는 경우, 개인정보 처리활동의 요구 사항을 충족하기 위한 가장 낮은 빈도를 채택해야 한다.

다. 공개 투명 원칙

「개인정보 보호법」 제7조에 따르면, 개인정보를 처리함에 있어 공개적이고 투명한 원칙을 준수해야 한다.

“공개□투명” 원칙은 개인정보처리자가 개인정보의 처리 규칙, 처리활동의 목적, 방법, 범위 등을 명확하고 알기 쉬운 방식을 통해 개인정보 주체에게 공개적으로 고지함으로써 개인정보 주체의 알 권리와 선택권을 보장하고 개인정보 주체의 동의가 관련 사항에 대한 충분한 이해를 전제로 이루어진 진실하고 유효하며 자발적인 의사표시임을 보장하도록 한다.[7] 예를 들어, 기업이 APP을 운영하는 경우, 개인정보 주체에게 명확한 방식(예컨대 팝업창 등 방식)으로 「개인정보보호정책」(또는 「개인정보처리방침」)을 발송하여 개인정보 처리 상황을 고지해야 한다.

라. 정확성 원칙

「개인정보 보호법」 제8조에 따르면, 개인정보를 처리함에 있어 정확성 원칙을 준수해야 한다.

“정확성 원칙”이란 개인정보처리자가 개인정보의 처리 품질을 보장하여 개인정보 처리 품질 문제로 인해 개인정보 주체의 권익에 불리한 영향을 초래하지 않도록 하는 것을 의미한다.

---

7) 영미법상의 “informed consent”와 같은 맥락으로 이해할 수 있다.

유의 사항
정확성 원칙은 「개인정보 보호법」 제46조에서 정한 개인정보 주체의 정정권 및 제47조에서 정한 개인정보 주체의 삭제권에서 구현되고 있다. 실무상 기업은 (1) 수집 단계에서 개인정보의 정확성과 완전성을 보장하고 (2) 정기적인 점검 및 업데이트 시스템을 구축하고, 잘못된 데이터를 즉시 제거하고 정정하기 위한 합리적인 조치를 취해야 하며 (3) 개인정보 주체의 정정 및 삭제 요구에 적극 대응하고, 개인정보 주체가 정정권 및 삭제권을 행사할 수 있도록 합리적인 방법과 채널을 마련해야 한다[8]

.

마. 책임성 및 데이터 보안 원칙

「개인정보 보호법」 제9조에 따르면, 개인정보를 처리함에 있어 책임성 및 데이터 보안 원칙을 준수해야 한다. “책임성 및 데이터 보안” 원칙이란 개인정보 처리자는 처리되는 개인정보의 안전을 보장하고, 그 개인정보 처리활동에 대해 책임진다는 것을 의미한다.

① 기업이 「개인정보 보호법」 규정 및 요구 사항을 위반하는 경우 다음과 같은 법적 처벌이 있다.

i) 시정명령, 과징금 부과, 면허취소, 불법소득 몰수 등 행정처벌을 받게 되는바, 사안이 중대한 경우 기업에 대한 과징금은 최대 5,000만 위안(한화 약 92억원[9]) 또는 직전연도 매출액 5%에 상당하는 금액, 개인에 대한 과징금은 최고 100만 위안(한화 약 1억8400만원)까지 가능함. 이러한 벌금은 유럽 GDPR에 비해서도 높은 수준이기 때문에 한국기업으로서는 특히 유의하여야 할 필요가 있다.

ii) 개인정보 주체 등에 대해 손해배상을 해야 함.

iii) 범죄에 개인정보를 활용했을 경우 형사 처벌될 수 있으며, 특별히 중대한 사건의 경우 3년이상 7년이하 유기징역과 벌금이 부과될 수 있음

② 실무적으로 기업은 자체 위험부담을 평가하고 기술 및 기타 안전조치를 통해 개인정보의 기밀성, 무결성(안전성), 가용성을 보장함과 동시에, 개인정보 보호책임자를 조속히 지정하고 사내 준법관리 제도 및 조치를 구축하여 법에서 정한 바에 따라 개인정보 처리업무를 수행해야 한다.

8) 자세한 내용은 본 가이드북 제3장 개인정보 준법 구조의 제3.3절 개인정보 주체의 권리 중 제3항 정정권 및 보완권, 그리고 제4항 삭제권의 내용을 참조.

9) 한화로 환산한 금액은 환율에 따라 변동 가능. 이하 동일.

※ 한국법상 “개인정보 보호 원칙”

[한국 개인정보 보호법 제3조]

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 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 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.

제 3절 개인정보 주체의 권리

「개인정보 보호법」 제44조 ~ 제49조에 따르면, 개인정보 주체는 다음과 같은 권리를 보유한다.

가. 알 권리와 결정권

자신의 개인정보를 기업이나 개인이 취급하고 있음을 알고 있어야 하므로, 알 권리와 결정권은 개인정보 주체의 가장 핵심적인 권리이다. 개인정보 주체는 다음 사항에 대해 알 권리와 결정권을 보유한다.

① 개인정보 처리 가능 여부
② 개인정보 처리 목적과 이유
③ 개인정보 처리 방식
④ 처리되는 개인정보 유형 및 범위
⑤ 개인정보 처리기간

⑥ 개인정보가 어떤 상황에서 처리되는지
⑦ 개인정보 처리에 대한 제한 여부

상기 사항은 개인정보 주체가 결정할 수 있으므로, 기업은 개인정보를 수집할 때 「개인정보보호정책」을 통해 수집되는 개인정보의 처리목적, 처리방식, 수집범위, 처리 및 이용 권한, 개인정보의 이용 상황 또는 이용되는 경우 등을 명확하게 고지해야만 개인정보 주체의 알 권리와 결정권이 보장될 수 있다.

유의 사항
- 개인정보를 처리하기 전에 「개인정보 보호법」 제13조에서 정한 개인정보 주체의 동의가 필요하지 않은 경우[10]를 제외하고는 개인정보 주체의 동의를 얻어야 한다는 점을 유의해야 한다. - 「개인정보보호정책」에서 제품 및 서비스의 기능과 수집된 개인정보 및 이용목적이 서로 매칭되도록 기재해야 한다. 예를 들어, 다음과 같이 「개인정보보호정책」을 작성할 수 있다. "*귀하가 당사의 제품 또는 서비스를 사용하기 위해 당사의 웹사이트와 APP에 로그인하는 것을 선택하셨다면 당사에 필수 정보, 즉 계정정보와 휴대전화번호를 제공하거나 당사가 그러한 정보를 수집할 수 있도록 허용해야 합니다. 해당 정보는 당사가 귀하의 신원을 식별함으로써 귀하가 로그인하고 귀하의 정보를 표시하는 데 도움을 주기 위해 사용하게 됩니다.*" - 개인정보의 수집 범위를 설명할 때 불명확한 수집을 방지하기 위해 "등"과 같은 포괄적인 단어를 사용하지 않도록 주의해야 한다.

나. 열람권, 복제권 및 이전 청구권

「개인정보 보호법」 제45조에서는 개인정보 주체의 열람권, 복제권 및 이전 청구권을 규정하였다. 즉, 별도 규정이 없는 한, 개인정보 주체는 자신의 개인정보를 열람, 복제할 수 있는 권리를 갖는다. 아울러 국가네트워크정보 당국에서 정한 기준에 부합되는 경우, 개인정보처리자는 개인정보 주체의 요구에 따라 개인정보의 이전 경로를 제공해야 한다.

유의 사항
개인정보 주체의 권리행사를 보장하기 위해 다음의 요구사항을 충족시켜야 한다. - 제도적으로 또는 제품 측면에서 개인정보 주체가 정보를 열람할 수 있는 경로 또는 방법을 제공해야 한다. 예를 들어, App 또는 웹사이트에 "나의 정보"

10) 자세한 내용은 본 가이드북 제3장 개인정보 준법 구조의 제3.4절 개인정보 처리 규칙 제1항 개인정보 처리의 기본 근거를 참조.

메뉴를 설정해두고 해당 메뉴에 수집되는 모든 정보를 명시한다. - 개인정보 주체의 열람 요청에 대응할 수 있도록 적어도 다음의 개인정보에 대한 열람 방법을 제공해야 한다. (1) 기업이 보유하고 있는 개인정보 또는 개인정보의 유형. (2) 개인정보의 출처 및 처리목적. (3) 상기 개인정보를 취득한 제3자의 신원 또는 유형.

다. 정정권 및 보완권

「개인정보 보호법」 제46조에 따르면, 개인정보 주체가 자신의 개인정보가 정확하지 않거나 불완전하거나 또는 기타 사유로 정정, 보완이 필요한 경우 (1) 개인정보처리자가 제공하는 인터페이스, 팝업창 또는 기타 경로를 통해 정정, 보완하거나 또는 (2) 전화, 이메일을 통해 개인정보처리자에게 그러한 정보의 정정, 보완을 요청할 수 있다.

유의 사항
- 개인정보 주체가 개인정보를 정정, 보완할 수 있는 경로와 방법을 제공함으로써, 해당 개인정보 주체가 제때에 효과적으로 자신의 권리를 행사할 수 있도록 해야 한다. 예를 들어, 이용자가 언제든지 개인정보를 정정, 보완할 수 있도록 어플리케이션(App) 내 개인정보에 대한 수정 옵션을 제공해야 한다. - 개인정보 주체가 개인정보를 정정, 삭제하거나 이용자 계정을 해지했다는 이유로 (1) 불필요하거나 불합리한 조건을 설정한다거나 (2) 개인정보 주체에게 별도의 의무를 요구해서는 아니 된다.

라. 삭제권

“삭제권”이란 법령이나 양자 간에 합의한 상황이 발생한 경우 개인정보 주체가 개인정보처리자에게 개인정보를 삭제하도록 요청할 수 있는 권리를 의미한다. 「개인정보 보호법」 제47조에 따르면, 다음의 경우에 해당하는 경우, 개인정보처리자는 지체 없이 개인정보 주체의 개인정보를 삭제해야 한다. 만약 개인정보처리자가 법령에 따라 제때에 개인정보를 삭제하지 않을 경우, 해당 개인정보 주체는 개인정보처리자에게 즉시 개인정보를 삭제하도록 요구할 수 있다.

개인정보의 처리목적이 이미 실현되었거나, 실현할 수 없거나, 처리목적을 실현하기 위해 더 이상 필요하지 않은 경우

개인정보처리자가 더 이상 제품 또는 서비스를 제공하지 않는 경우 또는 저장기간이 만료된 경우

개인정보 주체가 개인정보 처리에 대한 동의를 철회한 경우
개인정보처리자가 법령을 위반하거나 약정을 위반하여 개인정보를 처리한 경우
법령에서 정한 기타 상황
또한, 개인정보 주체가 삭제권을 행사하고자 하는 경우 법률 및 행정법규에 따른 저장기간이 경과되지 않았거나 개인정보를 삭제하는 것이 기술적으로 어려운 경우, 개인정보처리자는 저장 및 필요한 보호조치 이외의 기타 개인정보 처리활동을 중단해야 한다.

유의 사항
개인정보를 처리할 때 다음 사항에 유의해야 한다. - 관련 법령의 규정과 양자가 합의한 약정 사항을 준수하고, 개인정보 보호법 제47에 명시된 상황이 발생하는 경우 해당 개인정보를 지체 없이 삭제해야 한다. - 어플리케이션(App)에 삭제 옵션, 버튼을 추가하거나 서비스 인터페이스에 기업의 이메일 주소를 명시하는 등 개인정보 주체가 기업에 개인정보 삭제를 요구할 수 있도록 적절한 방법과 경로를 제공해야 한다.

마. 철회권

「개인정보 보호법」 제15조에 따르면, 만약 개인정보처리자의 처리권한이 개인정보 주체의 동의에 기반하는 경우, 해당 개인정보 주체는 수시로 그러한 동의를 철회할 수 있는 권한을 보유한다. 아울러, 개인정보처리자는 개인정보 주체가 철회권을 행사할 수 있도록 간편하고 빠른 동의 철회 방법을 제공해야 한다. 개인정보 처리 동의의 철회와 관련하여 다음 사항을 유의할 필요가 있다.

① 철회 전의 유효성 인정: 개인정보 주체의 동의 철회는 철회 전에 개인정보 주체가 이미 동의하여 진행한 처리활동의 효력에는 영향을 미치지 않는다(「개인정보 보호법」 제15조).

② 철회로 인해 발생할 수 있는 제품 및 서비스의 지속적 제공에 관한 시나리오: 개인정보 주체가 동의를 철회할 경우 다음 두 가지 상황이 가능하다.

i) 동의를 철회한 개인정보가 제품 및 서비스를 제공함에 있어 필수 정보가 아닌 경우, 개인정보처리자는 개인정보 주체가 동의를 철회하였다는 이유로 제품 및 서비스의 제공을 거절해서는 안 된다.

ii) 동의를 철회한 개인정보가 제품 및 서비스를 제공함에 있어 필수 정보라면 개인정보처리자는 제품 및 서비스의 제공을 거절할 수 있다(「개인정보 보호법」 제16조).

iii) 삭제권 행사 여부: 만약 개인정보 주체가 개인정보처리자의 개인정보에 대한 처리권한을 철회하는 경우, 개인정보처리자는 관련 개인정보를 자체적으로 삭제해야 한다. 만약 개인정보처리자가 해당 정보를 삭제하지 않은 경우, 개인정보 주체는 그러한 정보를 삭제할 것을 요구할 수 있는 권리를 가진다(「개인정보 보호법」 제47조).

유의 사항
개인정보 주체의 철회권 행사와 관련하여, 당해 개인정보를 기반으로 푸시 광고를 하는 경우 개인정보 주체에게 푸시 광고에 대한 동의를 철회하는 방법도 제공해야 한다.

바. 해석 설명권

「개인정보 보호법」 제48조에 따르면, 개인정보 주체는 개인정보처리자에게 자신의 개인정보에 대한 처리규칙에 대해 해석하고 설명해 줄 것을 요구할 수 있다. 즉, 기업은 개인정보 주체가 기업의 개인정보 처리규칙에 대해 문의하는 경우 적시에 개인정보 처리규칙에 대해 해석하고 설명해야 한다.

유의 사항
기업은 개인정보 주체에 해석 및 설명할 때 다음 사항에 유의해야 한다. - 「개인정보보호정책」 및 「서비스 이용약관」에서 개인정보 처리 규칙과 내용에 대해 자세하게 명시하고 설명해야 한다. - 만약 개인정보 주체가 개인정보 처리규칙에 대해 추가 해석과 설명을 요청하는 경우, 기업은 온라인 상담원 응답, 이메일 주소, 전화 등의 간편하고 빠른 방식을 제공하여 개인정보 주체가 관련 요구 사항을 제기할 수 있도록 해야 한다.

사. 사망자의 개인정보에 대한 개인정보 처리권

「개인정보 보호법」 제49조에 따르면, 만약 개인정보 주체가 사망한 경우, 그의 가까운 친족[11]은 적법하고 정당한 이익을 전제로 사망자의 개인정보에 대해 열람, 복사, 정정 또는 삭제 등의 권리를 행사할 수 있다. 다만, 개인정보 주체가 생전에 자신의 개인정보 처리에 대한 의사를 정하였을 경우, 개인정보처리자는 강제성 법규정을 위반하지 않는 전제 하에 사망자의 의사를 존중하여 개인정보를 처리해야 한다.

11) 중국법상 '근친족(近親屬)'이라고 하며, 배우자, 부모, 자녀, 형제자매, 조부모, 외조부모, 손자녀, 외손자녀를 포함한다.

유의 사항
개인정보 주체가 사망한 후의 개인정보 처리권에 관련하여 다음 사항에 유의해야 한다. - 기업은 사망자 개인정보에 대한 심사제도를 구축하고 가까운 친족에 대한 신원확인 절차를 규범화해야 한다. - 기업은 개인정보 주체 사망 이후의 개인정보 처리에 관한 법령과 법 집행 사례를 모니터링 하고 이를 참고하여 관련 개인정보처리 준법 시스템을 정비할 필요가 있다.

소결 - 개인정보 주체의 권리 관련 유의 사항
- 개인정보 주체가 법적 권리를 행사하는 경우, 근무일 기준 30일 이내[12]대응할 것을 권장한다. - 기업이 인터랙티브 방식(예: 웹사이트, 모바일 인터넷 어플리케이션(App), 소프트웨어 등)을 이용하여 제품 또는 서비스를 제공하는 경우, 간편하고 빠른 인터랙티브 기능이나 옵션을 제공하여 개인정보 주체가 온라인에서 접근, 정정, 삭제, 동의철회, 계정해지 등 권리를 행사할 수 있도록 해야 한다. 예를 들어, 기업은 어플리케이션(App) 등에 (1) 개인정보에 접근하거나 이를 정정, 삭제할 수 있는 인터페이스를 제공하거나 (2) 개인정보 처리를 철회할 수 있는 버튼 등을 설정할 수 있다. - 개인정보 주체의 합리적인 권리행사 요구에 대해 개인정보처리자는 원칙적으로 수수료를 수취하지 않아야 한다. 다만, 일정한 기간 내에 여러 차례 반복적으로 요청하는 경우, 그 구체적 사정에 따라 개인정보처리자는 일정 금액의 비용을 청구할 수 있다. - 만약 기업이 개인정보 주체의 요청을 처리함에 있어 고액의 비용이 발생하거나 현저하게 어려운 사정이 존재하는 경우, 개인정보처리자는 개인정보 주체의 적법한 권익을 보장할 수 있는 대안을 제공해야 한다. - 관련하여 기타 확인이 필요한 사항은 「개인정보안전규범」 제8조를 참조하시기 바란다.

※ 한국법상 "정보주체의 권리"

[한국 개인정보 보호법 제4조]
정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다. 1. 개인정보의 처리에 관한 정보를 제공받을 권리 2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리 3. 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함한다. 이하 같다)을 요구할 권리 4. 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리 5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

12) 개인정보안전규범에서는 30일 내 대응할 것을 요구하고 있다(제8.7조 a)목).

제 4절 개인정보 처리 규칙

가. 개인정보 처리의 기본 근거

「개인정보 보호법」 제13조에 따라 개인정보처리자는 다음 각 호의 어느 하나에 해당할 경우에만 개인정보를 처리할 수 있다.

① 개인정보 주체의 동의를 얻은 경우

개인정보처리자가 개인정보 주체로부터 동의를 얻은 경우에는 개인정보 주체의 동의 범위 내에서 개인정보를 처리할 수 있다. 예를 들어, 개인정보 주체가 특정 기업의 위챗(Wechat) 내 어플리케이션(App) 에서 자신의 위챗 ID와 프로필 사진을 수집 및 저장하는 데 동의했다면, 해당 기업은 상기 두 가지 정보를 수집 및 저장할 수 있다.

② 계약을 통해 약정한 경우

i) 계약체결 또는 계약상 의무이행 시 반드시 개인정보 처리가 필요한 경우, 계약 당사자는 개인정보를 처리할 수 있다. 예를 들어, 홍길동이란 고객이 부동산임대업체의 어플리케이션(App) 을 이용하여 부동산임대계약을 체결하고자 할 경우, 부동산임대업체는 부동산임대시 필수로 제공해야 하는 개인정보(예: 성명, 신분증번호)를 수집할 수밖에 없다. 이때, 부동산임대업체가 홍길동의 개인정보를 수집하는 행위는 적법한 행위에 해당한다.

ii) 기업이 법에 의거하여 근로규정제도 제정, 단체근로계약 체결, 인적자원 관리를 위해 반드시 개인정보가 필요한 경우, 관련 개인정보를 수집할 수 있다. 예를 들어, 베이징에 위치한 한국기업이 현지 근로자와 단체근로계약을 체결하는 경우, 단체근로계약이 체결되었음을 보장하기 위해서는 필요한 개인정보를 수집해야만 하는데, 이때 기업이 근로자의 개인정보를 수집하는 행위는 적법한 행위에 해당한다.

③ 법적 요구 사항 또는 규정을 따르는 경우

i) 기업이 법적 책임 또는 의무를 이행하기 위해 반드시 개인정보를 수집해야만 하는 경우, 관련 정보를 수집할 수 있다. 예: (ㄱ) 한국기업이 베이징에 자회사를 설립하면서 법인대표를 선임하는 경우, 기업이 법령에 따라 법인대표의 개인정보를 수집하여 관련 정부기관에 제공하는 행위. (ㄴ) 게임

회사가 실명제와 중독예방 관련 법령에 따라 게임 유저의 신원정보를 수집하는 행위.

ii) 기업이 공중보건 비상사태에 대응하거나 비상 상황에서 자연인의 생명건강과 재산안전을 보호하기 위해 반드시 개인정보의 수집이 필요한 경우, 개인정보를 수집할 수 있다. 예를 들어, 코로나19 발생 후 정부기관이 개인정보 주체의 동의없이 직접 개인정보를 처리하는 행위는 이에 해당한다.

iii) 기업이 공공의 이익을 위해 신문보도, 여론 모니터링 등을 이행할 때, 합리적인 범위 내에서 개인정보를 처리할 수 있다.

iv) 기업이 합리적인 범위 내에서 개인정보 주체가 스스로 공개했거나 이미 합법적으로 공개된 개인정보를 처리하는 행위는 적법 행위에 해당한다. 예를 들어, 한국의 부동산업체가 중국 법원에서 신용불량자로 등록, 공시한 개인정보를 수집하여 사내 아파트 분양 시스템에 등록함으로써 당해 신용불량자가 부동산을 분양 받지 못하도록 분양 담당자에게 알리는 행위는 적법 행위에 해당한다.

앞서 언급한 개인정보 처리와 관련하여, 법적 근거는 매우 중요하며, 이러한 법적 근거에 부합되는 경우에만 개인정보 주체의 동의 없이 개인정보를 처리할 수 있다. 실생활에서 법적 요구 사항이나 규정에 따라 개인정보를 처리하는 경우는 상대적으로 드물다. 따라서, 일반적으로 기업이 개인정보를 처리할 때에는 해당 개인정보 주체의 동의를 얻거나, 개인정보 처리에 관한 계약을 체결하거나 또는 계약에 따른 의무를 이행하는 데 반드시 필요한 경우에 한해야 한다.

나. 일반적인 개인정보 처리 규칙

① 동의에 관해

「개인정보 보호법」 제14조, 제15조 및 제16조에 따르면, 기업의 개인정보 처리에 관한 법적 근거가 개인정보 주체의 동의를 기반으로 하는 경우, “동의”에 관하여 다음 규정과 요구 사항에 대해 유의해야 한다.

i) 반드시 개인정보 주체의 유효한 동의를 얻어야 한다. “유효한 동의”란 개인정보 주체가 관련 상황을 충분히 파악했다는 전제 하에 자발적이고 명확하게 동의한 것을 의미한다. 즉, 개인정보 주체는 개인정보의 처리에 관한 전체 내용을 알고 있어야 하며 개인정보 주체의 동의 의사 표시는

자발적이어야 한다.(개인정보 주체가 사기, 협박 등에 의해 동의한 것이 아니어야한다). 또한, 개인정보 주체의 동의 표시는 묵시적이 아닌 명시적으로 이루어져야 한다. 예를 들어, 위챗 이용자의 프로필 사진과 성별 정보를 수집할 때, 이용자가 자발적으로 "동의" 옵션을 클릭하면 개인정보 주체의 유효한 동의를 얻은 것으로 간주된다. 반대로 이용자가 자발적으로 클릭하는 것이 아닌 "본 서비스를 사용하는 행위를 이용자가 개인정보 수집에 동의한 것으로 간주한다"는 정도로만 제시하는 경우 이는 "유효한" 동의를 받은 것으로 보기 어렵다. 또한, 법률 및 행정법규에서 개인정보 처리에 대해 별도의 동의 또는 서면 동의를 요구하는 경우 관련 규정[13]을 준수해야 한다.

ii) 개인정보의 처리목적, 방법 또는 개인정보의 종류를 변경하는 경우 개인정보 주체로부터 다시 동의를 얻어야 한다. 예를 들어, 기업이 업무상 필요에 의해 개인정보 주체의 나이를 추가로 수집하고자 할 때, 해당 사실을 개인정보 주체에게 고지 후 새로 동의를 얻어야 한다.

iii) 동의에 의한 개인정보 처리 시, 해당 개인정보 주체는 상기 동의를 철회할 권리를 갖는다. 기업은 개인정보 주체가 앞서 언급한 개인정보 처리에 대한 동의를 언제든지 철회할 수 있다는 점을 유의해야 한다. 따라서 기업은 개인정보 주체가 동의를 철회할 수 있는 간편하고 빠른 방법이나 경로를 제공해야 한다. 다만, 개인정보 주체가 동의를 철회하기 전에 개인정보 처리자에 의해 이미 처리된 개인정보는 이와 같은 철회의 영향을 받지 아니한다.

iv) 개인정보처리자는 개인정보 주체가 동의를 철회했다는 이유로 해당 개인정보 주체에 제품이나 서비스의 제공을 거절해서는 안 된다. 다만, 개인정보 주체가 제품이나 서비스에 반드시 필요한 개인정보의 제공에 대한 동의를 철회한 경우, 기업은 해당 제품 또는 서비스 제공을 거절할 수 있다. 예를 들어, 모바일 어플리케이션(App)을 이용해 기차표 예매 서비스를 제공하는 기업으로서는 이용자의 신분증번호를 필수 정보로 제공받아야 하는데, 이용자가 해당 정보의 제공 동의를 철회하는 경우 기업은 서비스 제공을 거부할 수 있다.

13) "별도의 동의" 및 "서면 동의"의 정의와 유의 사항은 본 가이드북 제2장「개인정보 보호법」 상 주요 정의 제2.9절 서면동의 및 제2.10절 별도의 동의를 참조.

유의 사항
기업이 개인정보 주체의 동의 사항을 처리하는 경우, 다음 조치를 취할 것을 권장한다. - 유효한 동의를 얻기 위한 기준, 동의서 양식 및 심사 규정을 마련하여 개인정보 주체의 동의를 얻는 사항을 절차화, 표준화한다. - 자발적으로 동의를 철회할 수 있는 경로를 제공해야 한다. 예를 들어 (1) 모바일 어플리케이션(App) 내 클릭, 체크, 기입 등 옵션을 이용하여 개인정보 주체가 개인정보 처리에 대한 동의 여부를 스스로 선택할 수 있도록 하거나, (2) 웹사이트상 기능을 실행하는 것과 동일하게 간편하고 빠른 기능 끄기 옵션이나 경로를 제공한다.

② 고지 의무에 관해

「개인정보 보호법」 제17조에 따르면, “고지 의무”란 개인정보처리자가 개인정보를 처리하기 전에 간결한 방식과 알기 쉬운 언어로 정확하며 완전하게 개인에게 다음과 같은 정보를 고지해야 함을 의미한다.

· 개인정보처리자의 명칭(법인) 또는 성명(개인)과 연락처
· 개인정보의 처리목적과 처리방법 및 처리하는 개인정보의 종류와 보관기간
· 개인정보 주체가 관련 권리를 행사하는 방법 및 절차
· 기타 법률 및 행정법규에서 정하는 바에 따라 고지해야 하는 사항

다만, 「개인정보 보호법」 제18조에 따라 다음과 같은 두 가지 상황이 발생할 경우, 개인정보처리자는 개인정보 주체에게 개인정보 처리사항을 고지하지 않거나 고지를 연기할 수 있다.

· 법령에 따라 개인정보처리자가 개인정보 처리에 대해 비밀을 유지해야 하거나 고지할 필요가 없는 경우, 개인정보 주체에게 고지하지 않아도 된다. 예를 들어, 「개인정보 보호법」 제13조에서 정한 공공이익을 위한 신문보도, 여론 모니터링 등 행위가 이에 해당한다.
· 개인정보처리자는 개인정보 주체의 생명과 재산을 보호하는 과정에서 적시에 개인정보 처리사항을 고지할 수 없는 경우, 비상 상황이 해소된 후 개인정보 주체에게 상기 처리사항을 고지해야 한다. 예를 들어, 병원에서 환자에게 응급처치를 하기 위해 수혈이 필요한데 혈액 부족으로 해당 환자의 혈액형을 타 병원에 제공하여 혈액을 지원받는 행위가 이에 해당한다. 이와 같은 응급상황

발생 시, 병원은 개인정보 주체의 동의 없이 관련 개인정보를 타 병원에 직접 제공하여 적절한 혈액을 지원받을 수 있다.

유의 사항
고지 의무를 이행할 때 다음 사항에 유의해야 한다. - 기업은 개인정보 처리활동의 실제 상황에 따라 적시에 「개인정보보호정책」을 작성, 수정 및 갱신하고, 명확한 방식을 통해 개인정보 주체에게 고지해야 한다. - 만약 별도의 동의가 필요한 경우, 기업은 명확한 별도의 방식(예: 어플(App) 내 별도 팝업창)을 통해 적시에 개인정보 주체에게 고지하여 별도의 동의를 얻어야 한다.

③ 최소 보관에 관해

「개인정보 보호법」 제19조에 따르면, “최소 보관”이라 함은 개인정보의 처리목적을 실현함에 있어 필요한 최단 시간 동안만 개인정보를 보관한다는 것을 의미한다.

유의 사항
- 개인정보를 처리한 후 관련 개인정보를 계속해서 보관할 필요가 없을 경우, 제때에 삭제하거나 익명화 처리를 해야 한다. - 개인정보의 보관 및 파기 규정, 지침 등 내부 규정을 제정하여 개인정보의 보관과 삭제에 대한 체계적인 관리 제도를 마련할 수 있다. 다만, 법령에서 최단 보관기간을 정한 경우에는 예외로 한다(예: 「전자상거래법」 제31조에서는 “제품 및 서비스 정보, 거래정보의 보관기간은 거래 완료일로부터 3년 이상으로 하며, 법률 및 행정법규에 달리 규정한 경우에는 해당 규정을 따른다”고 규정하고 있다. 따라서 기타 법령에 달리 규정된 경우를 제외하고 상기 제품 및 서비스 정보, 거래정보에 해당하는 개인정보도 「전자상거래법」에 따라 3년 이상 보관해야 한다).

다. 개인정보 처리에 관한 특별 규정

① 공동처리

「개인정보 보호법」 제20조에 따르면, “공동처리”란 2인 이상의 개인정보 처리자가 개인정보를 공동으로 처리하는 것을 의미한다. 이 경우 개인정보 처리자는 개인정보의 처리목적과 처리방법을 공동으로 결정해야 하며, 각자의 권리와 의무를 명확하게 약정해야 한다. 다만, 공동으로 처리할 사항을 약정함에 있어 개인정보 주체가 임의의 개인정보처리자에게 「개인정보 보호법」에 따른 권리를 행사하는 데 영향을 미치지 않도록 유의해야 한다. 또한, 개인정보의 공동처리로 인해 개인정보 주체가 피해를 입은 경우, 개인정보처리자들은 연

대하여 공동으로 책임을 부담해야 한다.

유의 사항
기업이 개인정보를 공동으로 처리하는 경우, 다음 사항에 유의해야 한다. - 기업이 타 업체와 공동으로 개인정보를 처리하고자 하는 경우, 공동 처리하는 협력사에 대해 사전 평가를 진행할 필요가 있으며, 적법하고 평판이 양호한 협력사를 선정해야 한다. - 공동 개인정보처리자와 서면 계약을 체결하여 개인정보를 공동으로 처리하는 목적, 방법, 양자간의 권리 및 의무를 명시적으로 정해야 한다. - 「개인정보보호정책」과 관련 문서를 검토하여 개인정보를 공동으로 처리하는 처리자의 명칭, 처리목적, 처리방법, 처리범위 및 처리자별 권리와 의무를 이미 개인정보 주체에게 명확하게 고지했는지 여부를 체크해야 한다.

② 위탁처리

「개인정보 보호법」 제21조에 따르면, “위탁처리”란 개인정보처리자가 개인정보 처리에 관한 사항을 제3자에게 위탁하여 처리하는 것을 의미한다. 다양한 시나리오와 역할에 따라 기업은 개인정보 처리의 위탁자일 수 있고 수탁자일 수도 있다.

i) 개인정보 처리 위탁자의 의무

「개인정보 보호법」 제21조에 따라 개인정보 처리 위탁자는 다음의 의무를 이행해야 한다.

· 위탁 내용에 관한 의무 명문화: 개인정보 처리 위탁자는 위탁 처리의 목적, 기간, 처리방법, 개인정보의 종류, 보호조치 및 양자의 권리와 의무 등을 명확히 해야 한다. 아울러 이러한 내용들을 위탁계약서에도 명시적으로 약정할 것을 권장한다.

· 감독의 의무: 개인정보 처리 위탁자는 수탁자의 개인정보 처리활동에 대해 감독해야 한다. 예를 들어, 개인정보 처리 위탁자는 수탁자의 개인정보 처리활동에 대해 정기적인 감사를 진행할 수 있다.

ii) 개인정보 처리 수탁자의 의무

「개인정보 보호법」 제21조와 제59조에 따라 개인정보 처리 수탁자는 다음의 의무를 이행해야 한다.

· 약정에 따라 개인정보를 처리: 개인정보 처리 수탁자는 위탁자와의 약정에 따라 개인정보를 처리해야 하며, 약정된 개인정보 처리의 목적, 방법 및 범위를 벗어나서는 아니 된다.

· 위탁계약서 무효 시의 특별 의무: 개인정보 처리 관련 계약이 무효이거나 효력이 발생하지 않거나 또는 철회, 해지된 경우, 개인정보 처리 수탁자는 모든 개인정보를 개인정보처리자(위탁자)에게 반환하거나 삭제해야 하며 보관하지 말아야 한다.

· 필요한 조치를 통한 개인정보 안전 보장 의무: 개인정보 처리 수탁자는 「개인정보 보호법」과 기타 법령에 따라 처리하는 개인정보를 안전하게 관리해야 한다.

· 이행 협조의 의무: 개인정보 처리 수탁자는 위탁자가 「개인정보 보호법」에 따른 의무를 이행하는 데 협조해야 한다. 예를 들어, 개인정보 주체가 권리를 행사하는 경우, 수탁자는 위탁자의 상기 권리행사 대응에 협조해야 한다.

유의 사항
개인정보 처리를 위탁할 때 다음 사항에 유의해야 한다. - 개인정보처리자는 수탁자에게 개인정보 처리사항을 위탁하기 전에 「개인정보 보호법」 제55조 및 제56조에 따라 미리 개인정보보호 영향평가를 실시하고 처리 상황을 기록해야 한다. - 위탁자는 「개인정보보호정책」 관련 문서를 검토하여 개인정보 주체에게 수탁자의 유형 또는 신원 등 기본 정보와 개인정보 처리의 목적, 방법 및 범위를 명확하게 고지해야 한다. - 개인정보 처리 위탁자와 수탁자가 체결한 서면 계약서에 약정된 개인정보 처리 내용은 「개인정보보호정책」에서 개인정보 주체에게 공개한 내용과 일치해야 한다. - 위탁자는 수탁자의 개인정보 처리활동을 감독하는 동시에, 개인정보 처리에 관한 위탁 상황을 정확하게 기록하고 보관해야 한다. - 위탁자는 수탁자가 위탁한 요구 사항에 따라 개인정보를 처리하지 않거나 개인정보의 안전한 보호 책임을 이행하지 않음을 발견하는 경우, 즉시 수탁자에게 개인정보 처리활동을 중단하도록 해야 한다. 또한, 수탁자가 합리적이고 유효한 구제 조치(예: 비밀번호 변경, 권한철회, 네트워크 연결 차단 등)를 취하도록 조치하거나 요구해야 한다.

③ 제3자 제공

「개인정보 보호법」 제22조와 제23조에 따르면, 제3자에게 개인정보를 제공하는 경우는 다음과 같이 두 가지 경우가 있다.

i) 자발적으로 다른 개인정보처리자에게 개인정보를 제공하는 경우(제23조):

개인정보처리자가 상업적 이유나 경영상 필요로 인해 자신이 수집한 개인정보를 자발적으로 제3자에게 제공하는 것을 가리킨다. 이 경우, 기존의 개인정보처리자는 개인정보를 이전 받는 자의 명칭, 연락처, 개인정보 처리의 목적, 방법 및 개인정보의 종류를 관련 개인정보 주체에게 고지해야 하며, 「개인정보 보호법」에 따라 개인정보 주체로부터 별도의 동의를 얻어야 한다. 개인정보를 이전 받는 자는 개인정보 주체가 동의한 범위 내에서만 개인정보를 처리할 수 있으며, 처리의 목적, 방법 또는 개인정보의 종류 등 그 범위를 변경하고자 하는 경우, 「개인정보 보호법」과 관련 법령에 따라 개인정보 주체로부터 다시 별도의 동의를 얻어야 한다.

ii) 수동적으로 다른 사람에게 개인정보를 제공하는 경우(제22조): 개인정보처리자의 자체 상황 변화로 인해 개인정보를 제3자에 제공해야 하는 경우를 가리킨다. 예를 들어, 기업의 합병, 분할, 해산, 파산선고 등의 경우가 이에 해당한다. 이 경우, 기존의 개인정보처리자는 개인정보를 이전 받는 자의 명칭 또는 성명, 연락처 등을 개인정보 주체에게 고지해야 한다. 아울러, 개인정보를 이전 받는 자가 개인정보의 처리 목적, 방법 또는 범위를 변경하고자 하는 경우, 「개인정보 보호법」과 관련 법령에 따라 개인정보 주체로부터 다시 별도의 동의를 얻어야 한다.

유의 사항
개인정보를 자발적으로 제공하든 수동적으로 제공하든 불문하고 다음 사항에 유의해야 한다. - 제3자에게 개인정보를 제공하는 경우, 기업은 「개인정보 보호법」 제55조 및 제56조에 따라 개인정보 영향평가를 실시[14]해야 한다. 즉, 개인정보를 제공한 후의 위험에 대해 평가하여 효과적인 보호조치를 취해야 한다. - 기업은 「개인정보보호정책」에서 공개하거나 고지한 제3자에게 개인정보 제공 관련 내용이 「개인정보 보호법」의 규정에 적합한지 여부를 검토해야 한다. 아울러, 개인정보 주체로부터 별도의 동의를 얻어야 하는 경우, 제때에 개인정보 주체에게 고지하고 별도의 동의를 얻어야 한다. - 만약 기업이 해산 또는 파산하여 개인정보를 이전 받을 자가 없는 경우, 모든 개인정보를 제때에 삭제하거나 익명화 처리하여 유출을 방지해야 한다.

④ 개인정보 자동화 의사결정

「개인정보 보호법」 제24조에 따라 개인정보처리자가 자동화 의사결정을 채택

14) 개인정보 영향평가에 관해서는 본 가이드북 제3장 개인정보 준법 구조 제3.5절 기업의 의무 중 제4항 개인정보보호 영향평가 의무 부분을 참조.

하는 경우, 다음 세 가지 사항에 유의해야 한다.

i) 개인정보처리자는 자동화 의사결정의 투명성과 결과의 공평성 및 공정성을 보장해야 하며, 개인을 상대로 거래가격에 대해 부당한 차별대우를 적용해서는 아니 된다. 다시 말해, 기업은 소비자를 상대로 자동화 의사결정을 이용한 "빅데이터 기반의 기존 소비자에 대한 차별대우(大数据杀熟)"와 "빅데이터 기반의 신규 소비자에 대한 차별대우(大数据杀生)" 등 행위를 해서는 아니 된다.

ii) 개인정보처리자는 개인을 상대로 정보를 푸시하거나 상업적 마케팅을 진행할 때 개인 특성을 이용하여 자동화 의사결정을 하지 않는 옵션이나 간편하고 빠른 거절 방식을 함께 제공해야 한다. 즉, 개인정보처리자가 자동화 의사결정 방식을 이용하여 정보를 푸시할 때 개인정보 주체가 언제든지 거절할 수 있어야 한다. 예를 들어, 기업은 자사 어플리케이션(App)에 자동화 의사결정 해제 버튼을 설정하여 개인정보 주체가 자동화 의사결정 기능을 편리하게 해제할 수 있도록 해야 한다.

iii) 만약 개인정보처리자의 자동화 의사결정 방식에 의한 개인정보 처리활동이 개인정보 주체에게 중대한 영향을 미치는 경우, 개인정보 주체는 개인정보 처리자에게 설명을 요구할 수 있는 권리를 가진다.

유의 사항
자동화 의사결정과 관련하여 다음 사항에 유의해야 한다. - 자동화 의사결정을 적용하기 전에 「개인정보 보호법」 제55조 및 제56조에 따라 개인정보보호 영향평가를 실시하고, 평가 결과에 따라 상응하는 조치를 취해야 한다. - 자동화 의사결정을 적용할 때 자동화 의사결정 콘텐츠와 비자동화 의사결정 콘텐츠를 명확하게 구분해야 한다. 예를 들어, (1) 자동화 의사결정 콘텐츠에 "타겟 푸시(定推)" 등 문구를 명시하거나 (2) 다양한 카테고리, 섹션, 페이지 등을 통해 달리 표시할 수 있다. - 기업이 자동화 의사결정 서비스를 제공하는 과정에서 자동화 의사결정 표시가 의존하는 태그에 대한 자율적인 제어 메커니즘(예: 태그 등 다중 ON/OFF 버튼)을 구축하여 개인정보 주체가 자동화 의사결정 수준을 조정할 수 있는 권리를 보장할 것을 권장한다.

⑤ 개인정보의 공개

「개인정보 보호법」 제25조에 따라 개인정보처리자는 개인정보 주체로부터

별도의 동의를 얻지 않는 한 일반적으로 개인정보를 공개할 수 없다.

유의 사항
기업에서 개인정보를 공개하는 경우, 다음 사항에 유의해야 한다. - 기업이 「개인정보 보호법」 제13조 제1항 제(2)호 내지 제(7)호에 규정된 사유에 따라 개인정보를 공개하는 경우, 개인정보 주체로부터 별도의 동의를 얻을 필요가 없다. - 기업이 법에 따라 개인정보를 공개하고자 하는 경우, 개인정보 공개로 인한 분쟁과 쟁의를 방지하기 위해 개인정보 공개에 관한 절차 및 검토 시스템을 구축하는 것이 바람직하다. - 개인정보 공개 시 개인정보 주체로부터 별도의 동의를 얻어야 한다는 점에 비추어, 기업은 개인정보 공개 사항에 관해 즉시 개인정보 주체에게 이메일을 발송하거나 어플리케이션(App) 내에서 별도 통지하는 방식으로 개인정보 주체에게 고지할 것을 권장한다. 아울러, 별도의 동의 방식과 관련하여 업계의 실제 운영사례에 대해 관심을 가지고 살펴볼 필요가 있다.

⑥ 공공장소에서의 영상 수집

「개인정보 보호법」 제26조에 따르면, 공공장소에 영상수집 장치(CCTV 등)나 개인 신원식별 장치를 설치하는 경우 ① 국가의 관련 법령을 준수하고, ② 공공안전을 유지하기 위한 필수적 조치임을 전제로 하며, ③ 명확한 안내 표지가 설치되어야 한다. 또한, 수집된 개인 영상이나 신원식별 정보 등은 공공안전을 유지하기 위한 목적으로만 사용되어야 하며 타 용도로 사용되어서는 안 된다. 다만, 개인정보처리자가 개인정보 주체로부터 별도의 동의를 얻은 경우에는 앞서 언급한 영상과 정보를 타 용도로 처리할 수 있다.

유의 사항
기업이 공공장소에서 영상을 수집해야 하는 경우 다음 사항에 유의해야 한다. - 해당 공공장소에 설치된 영상수집 및 개인 신원식별 장치를 점검하고 개인정보의 수집 목적을 정비하며, 관련 장치 근처에 선명한 안내 표지를 부탁하여 개인정보 주체에게 영상수집 구역에 진입하였음을 알린다. - 만약 영상수집 또는 개인 신원식별 장치가 공공안전을 유지하기 위해 필요한 것이 아니라면, 즉시 철거해야 함과 동시에 이미 수집된 개인정보를 삭제하거나 익명화 처리할 것을 권장한다. 단, 개인정보 주체로부터 별도의 동의를 얻은 경우는 예외로 한다.

⑦ 공개된 개인정보의 이용

「개인정보 보호법」 제27조에 따르면, 개인정보처리자는 개인이 스스로 공개했거나 이미 적법한 절차에 따라 공개된 개인정보를 합리적인 범위 내에서 처리할 수 있다. 다만, 개인정보 주체가 이미 공개된 개인정보의 이용을 명확하게 거절하는 경우, 개인정보처리자는 상기 정보를 처리해서는 아니 된다. 만약 개인정보처리자가 이미 공개된 개인정보를 처리하는 행위가 개인정보 주체의 권익에 중대한 영향을 미치는 경우 별도의 동의를 얻어야 한다.

유의 사항
기업이 공개된 개인정보를 처리하는 경우 다음 사항에 유의해야 한다. - 공개된 개인정보의 출처를 분석하고, 공개 사유가 적법하고 규정에 부합되는지 여부를 확인하며, 공개된 개인정보의 합리적인 처리범위를 정하고, 개인정보 주체의 권익에 미치는 영향을 평가해야 한다. - 공개된 개인정보의 합리적인 이용 범위에 관한 법령과 실제 법 집행 과정의 학계 논리 또는 실제 사례에 대해 관심을 갖고 살펴볼 필요가 있으며, 특히 개인정보침해죄[15]에 관한 사례에 주의를 기울여야 한다. 아울러, 학계의 논리 및 사례를 기반으로 기업 내 공개된 개인정보의 처리 시스템, 절차, 방법에 대해 제때에 조정 및 시정해야 한다.

⑧ 민감 개인정보의 처리

첫째, 「개인정보 보호법」 제28조에 따르면, 민감 개인정보는[16] 유출되거나 불법으로 이용되면 쉽게 개인정보 주체의 인격 존엄성을 침해하거나 신체적•금전적 안전을 해칠 수 있으므로, 개인정보처리자는 ① 특정 목적과 필요성이 있는 경우와 ② 엄격한 보호조치를 취한 경우에 한하여 민감 개인정보를 처리할 수 있다.

둘째, 「개인정보 보호법」 제29조에 따르면, 개인정보처리자는 민감 개인정보를 처리함에 있어 개인정보 주체로부터 별도의 동의를 얻어야 한다. 더불어, 법령상 민감 개인정보 처리시 관련 주체의 서면동의를 얻도록 규정한 경우, 상기 주체로부터 서면 동의를 얻어야 한다.

유의 사항 (1)
기업은 취급하는 민감 개인정보의 종류를 불문하고 향후 법적 위험을 피하기 위해 민감 개인정보 처리 시에는 개인정보 주체로부터 서면으로 동의를 받아둘 것을 권장한다.

15) 중국 형법 제253조의 1

16) 민감 개인정보의 정의는 본 가이드북 제2장「개인정보 보호법」 상 주요 정의 제2.2절 민감 개인정보의 내용을 참조.

셋째, 「개인정보 보호법」 제30조에 따르면, 개인정보처리자는 민감 개인정보를 처리함에 있어 개인정보 주체에게 제17조의 관련 사항[17]을 고지해야 하는 것은 물론, 추가로 민감 개인정보 처리의 필요성과 개인정보 주체에 미치는 영향도 고지해야 한다.

유의 사항 (2)
민감 개인정보를 처리할 때 개인정보 주체에게 다음 사항을 고지해야 한다. - 개인정보처리자의 명칭(법인) 또는 성명(개인)과 연락처 - 개인정보의 처리목적과 처리방법 및 처리하는 개인정보의 종류와 보관기간 - 개인정보 주체가 관련 권리를 행사하는 방법 및 절차 - 민감 개인정보 처리의 필요성과 개인정보 주체에게 미치는 영향 - 기타 법령에서 요구하는 사항

마지막으로, 「개인정보 보호법」 제31조에 따르면 개인정보처리자가 만 14세 미만 미성년자의 개인정보를 처리해야 하는 경우[18], 부모 또는 보호자(후견인)의 동의를 얻어야 한다. 더불어 앞서 언급한 동의 외에 만 14세 미만 미성년자를 대상으로 하는 별도의 개인정보처리규칙을 마련하고 시행해야 한다.

유의 사항(3)
민감 개인정보를 처리할 때 다음 사항에 유의해야 한다. - 자사가 민감 개인정보 처리에 관여하는지 여부를 파악하고, 만약 민감 개인정보를 처리해야 하는 경우에는 실제 상황에 따라 보다 높은 수준의 보호 시스템과 정책을 수립해야 한다. - 민감 개인정보를 전송하거나 보관할 경우, 암호화와 같은 보안조치를 취해야 한다. - 개인의 생체인식 정보를 처리할 때 다음 사항에 유의해야 한다. ① 개인의 생체인식 정보는 개인 신원 정보와 구분하여 보관한다. ② 개인 생체인식 원본 정보(예: 샘플, 영상 등)는 원칙적으로 보관하지 말아야 하며, 이때 다음의 조치를 취할 수 있다. (i) 개인 생체인식 요약 정보(요약 정보는 흔히 되돌릴 수 없는 특성이 있어 원본 정보를 역추적할 수 없다)만 보관한다. (ii) 수집 단말기에서 직접 개인 생체인식 정보를 이용하여 신원식별, 인증 등 기능을 구현한다. (iii) 안면인식, 지문, 손금, 홍채 등을 이용하여 신원 인증 등 기능을 구현한 후에는 개인 생체인식 정보를 직접 추출할 수 있는 관련 원본 영상을 삭제해야 한다.

17) 본 가이드북 제3장 개인정보 준법 구조 제3.4절 개인정보 처리 규칙 중 제2항 일반적인 개인정보 처리 규칙의 (2) 고지의 의무과 관련된 내용을 참조.

18) 만 14세 미만의 아동에 대해서는 「아동개인정보 인터넷 보호규정」 (儿童个人信息网络保护规定)이 적용됨을 유의할 필요가 있다.

- 만 14세 미만 미성년자를 대상으로 한 개인정보처리규칙을 별도로 마련해야 한다. 예를 들어, 「서비스 이용약관」 또는 「개인정보보호정책」에 “만 14세 미만의 미성년자인 경우, 서비스 이용 전 반드시 부모님이나 법정보호자(후견인)의 동의를 받으셔야 합니다”를 명시하고, 만 14세 미만 미성년자를 대상으로 한 별도의 「개인정보보호정책」을 첨부해야 한다.

제 5절 기업의 의무

「개인정보 보호법」 제5장에 따르면, 개인정보처리자는 개인정보보호 관련 요구사항을 충족하기 위해 다음과 같은 의무를 준수해야 한다.

가. 기본 의무

「개인정보 보호법」 제51조에 따르면, 개인정보처리자는 개인정보의 처리 목적, 방법, 종류 및 개인의 권익에 미치는 영향, 잠재적 위험성 등에 따라 개인정보 처리활동이 법령에 적합하도록 하는 동시에 무단 접근, 개인정보의 유출, 변조 및 분실 상황이 발생하지 않도록 하기 위해 다음과 같은 조치를 취해야 한다.

① 내부 개인정보 준법관리 제도와 운영절차를 마련해야 한다. 이에는 개인정보 준법관리 규칙, 개인정보 처리 운영절차 및 기타 규정과 제도를 포함하되 이에 국한되지 않는다.

② 개인정보를 범주별로 구분하여 관리해야 한다. 현재 금융, 공업 및 기타 업계에서는 이미 산업데이터에 대한 범주 및 등급 분류 기준 또는 지침을 마련하였다. 예를 들어, 「JR/T 0171-2020 개인금융정보 보호기술 규범」에서는 개인금융정보를 C3, C2, C1 세 가지 범주로 분류하고 있으며, 종류별 개인금융정보에 대해 서로 다른 수준의 관리와 보호조치를[19] 채택하고 있다.

③ 암호화, 비식별화 등 보안기술 조치를 취해야 한다. 개인정보처리자는 기술적 조치를 취할 때 개인정보의 범주 분류 결과, 개인의 권익에 미치는 영향, 잠재적 보안 위험성 등을 감안하여 필요하고 합리적인 기술적 조치를 취해야 한다.

④ 개인정보 처리에 대한 운영 권한을 정하고, 정기적으로 종사자에 대한 안전 교육 및 훈련을 실시해야 한다. 아울러 기업이 다음과 같은 조치를 취할

19) 자세한 내용은 본 가이드북 제4장 업무 유형별 개인정보보호 대응 방법 제4.5조 금융서비스 제공 시나리오 제1항 개인금융정보 범주 및 등급 분류의 (3) 표준별 개인금융정보 분류를 참조.

것을 권장한다. i) 개인정보처리자는 개인정보취급자의 범위와 개인정보 보안에 대해 총괄하여 책임을 부담하는 법인대표 또는 주요 책임자를 명확히 정할 것. ii) 개인정보에 대한 운영절차, 내부 접근 및 처리 시스템에 관한 지침과 요구 사항을 표준화하고 개인정보 처리와 관련된 활동을 기록할 것. iii) 개인정보취급자와 비밀유지계약을 체결하고 연 1회 이상 정기적인 교육을 실시할 것.

유의 사항
- 「개인정보 보호법」에 규정된 기본 의무를 이행하기 위해 개인정보 준법관리 시스템을 구축할 때 다음 사항을 포함해야 한다. ① 개인정보 처리(수집•전송•보관•공유 등을 포함) 행위의 전체 생애주기에 관한 규정 ② 담당부서 및 취급자의 운영절차, 개인정보 처리 권한 ③ 개인정보 보안사건에 대한 비상대책. - 기업이 개인정보에 관한 준법교육을 실시할 때 개인정보보호에 관한 인식 교육과 제도에 관한 실천훈련을 포함해야 하며, 사내 교육 대상에는 경영진, 업무, 기술, 법무 및 준법감시인이 포함되어야 한다.

나. 개인정보보호 책임자 지정 또는 기구 설립의 의무

「개인정보 보호법」 제52조에 따르면, 중국 국내에 있는 개인정보처리자가 처리하는 개인정보 수량이 국가네트워크정보 당국에서 정한 기준에 도달하는 경우, 개인정보보호책임자를 지정하여 개인정보 처리활동과 보호조치 등에 대해 감독 책임을 부담하도록 해야 한다. 아울러, 개인정보처리자는 개인정보보호책임자의 연락처를 공개하고 그의 성명, 연락처 등을 개인정보보호업무를 수행하는 담당부서에 신고해야 한다.

「개인정보 보호법」 제53조에 따르면, 국외에 위치한 개인정보처리자는 중국 내에 전문 기구를 설립하거나 대표자를 지정하여 개인정보보호업무를 책임지도록 해야 한다. 또한, 해당 기구의 명칭 또는 대표자의 성명, 연락처 등을 개인정보보호업무를 수행하는 담당부서에 신고해야 한다. 즉, 한국에 소재한 기업이 중국인의 개인정보를 처리해야 하는 경우, 중국 국내에 전문 기구를 설립하거나 대표자를 지정하여 법적 요구 사항에 따라 해당 대표자의 개인정보를 공개 및 신고해야 한다.

유의 사항
- 「개인정보안전규범」 (GBT35273-2020)에 따라 다음과 같은 조건에 해당하는 기업은 개인정보보호 책임자와 전문 기구를 설치할 것을 권장한다. ① 주요 업무가 개인정보 처리에 해당하며 직원수가 200명 이상인 경우. ② 100만 명 이상의 개인정보를 처리하거나 12개월 이내에 100만 명 이상의 개인정보를 처리할 것으로 예상되는 경우.

③ 10만 명 이상의 민감 개인정보를 처리하는 경우. - 실무상 개인정보보호 책임자와 전문 기구는 다음과 같은 업무를 책임지고 수행할 것을 권장한다. ① 사내 개인정보 보안 업무를 총괄 지휘하고 그에 대해 직접적인 책임을 부담. ② 개인정보보호 업무계획을 수립하고 그 이행을 감독. ③ 개인정보보호 정책, 절차, 규정을 제정, 배포, 시행 및 정기적으로 업데이트. ④ 기업이 보유하고 있는 개인정보 목록과 접근권한 정책을 수립, 유지 및 업데이트. ⑤ 개인정보 영향평가를 실시하고 잠재적인 보안 위험에 대한 개선 작업을 감독. ⑥ 정기적으로 개인정보 보안 교육을 실시. ⑦ 제품이나 서비스를 정식으로 오픈하기 전에 테스트 작업을 수행. ⑧ 불만사항의 제출 방법 및 신고 방법 등을 신속하게 공개하고 불만사항 및 신고사항을 신속하게 수리. ⑨ 정기적으로 개인정보 보안 감사 작업을 실시. ⑩ 개인정보보호 감독당국과 소통을 유지하고, 개인정보보호사건의 조치 상황을 제때에 보고.

다. 개인정보 처리에 대한 준법감사 의무

「개인정보 보호법」 제54조에 따르면, 개인정보처리자는 자체 개인정보 처리활동이 법령에 부합되는지 여부에 대해 정기적으로 준법감사를 실시해야 한다.

유의 사항
- 개인정보 처리활동에 대해 정기적인 준법감사는 이행조치에 대한 감사와 보안감사 두 가지로 나뉜다. 기업은 준법감사를 실시할 때 법령을 준수하고 있는지에 초점을 둘 필요가 있으며 감사 진행 시 개인정보보호 정책, 규정, 절차 및 안전조치의 유효성을 감사해야 한다. - 기업은 자동감사 시스템을 구축하여 개인정보 처리활동을 모니터링하고 기록할 수 있다. - 감사보고서와 관련 내용은 향후 보안사건 처리, 비상사태 대응 및 사후조사의 근거로 제공하기 위해 적절하게 보관해야 한다.

라. 개인정보보호 영향평가의 의무

「개인정보 보호법」 제55조에 따르면, 다음 각 호의 어느 하나에 해당하는 경우 개인정보처리자는 사전에 개인정보보호 영향평가를 실시하고 개인정보 처리 상황과 결과를 기록해야 한다.

① 민감 개인정보를 처리하는 경우

② 개인정보를 이용하여 자동화 의사결정을 진행하는 경우

③ 개인정보를 위탁 처리하거나 제3자 개인정보처리자에게 개인정보를 제공하거나 개인정보를 공개하는 경우

④ 중국 국외에 개인정보를 제공하는 경우

⑤ 개인정보 처리활동이 개인의 권익에 중대한 영향을 미치는 경우

아울러 「개인정보 보호법」 제56조에 따라 개인정보보호 영향평가 보고서와 처리상황 기록을 3년 이상 보관해야 한다. 나아가, 앞서 언급한 보고서와 기록에는 다음의 내용이 포함되어야 한다. i) 개인정보의 처리목적, 처리방법 등의 적법성, 정당성, 필요성. ii) 개인정보 주체의 권익에 미치는 영향 및 보안 위험성. iii) 개인정보 처리에 관한 보호조치가 적법하고 효과적인지, 위험 수준에 적합한지 여부.

유의 사항
개인정보보호 영향평가 시스템을 구축할 때 다음 사항에 유의해야 한다. - 개인정보보호 영향평가 시나리오를 파악한다. - 개인정보보호 영향평가에는 개인정보 처리 목적과 방법, 개인의 권익에 미치는 영향 및 보안 위험성, 안전 보호조치가 포함되어야 한다. - 개인정보보호 영향평가 및 위험 처리 상황을 기록해야 한다.

마. 개인정보 보안사건에 대한 적절한 처리의 의무

「개인정보 보호법」 제57조에 따르면, 개인정보의 유출, 변조, 분실이 발생하거나 발생할 우려가 있는 경우, 개인정보 처리자는 즉시 구제 조치를 취하고 개인정보보호업무를 수행하는 담당부서와[20] 개인정보 주체에게 통지해야 하며, 통지 내용에는 다음 사항을 포함해야 한다.

① 개인정보의 유출, 변조, 분실이 발생했거나 발생할 우려가 있는 정보의 종류, 원인 및 가능한 피해
② 개인정보처리자가 취한 구제 조치 및 개인정보 주체의 피해를 줄이기 위해 취할 수 있는 완화 조치
③ 개인정보처리자의 연락처

개인정보 보안사건의 위해성이 낮고 개인정보처리자가 취한 조치가 정보의 유출, 변조, 분실로 인한 피해를 효과적으로 방지할 수 있는 경우, 해당 개인정보 주체에게 통지하지 않아도 된다. 다만, 개인정보보호업무를 수행하는 담당부서가 피해 우려가 있다고 판단하는 경우, 개인정보처리자에게 통지할 것을 요구할 수 있다. 다만, 「개인정보 보호법」에서 통지 방식에 대한 규정을 두고 있지 않으므로 개인정보처리자는 실제 상황에 따라 전화, 이메일 등 1대1 통지 방식 또는 공고 등 대체 통지방식을 선택할 수 있으나 추후 통지 방식을 규정하는 법규가 공포되는지 여부를 모니터링하고 살펴볼 필요가 있다.

20) 개인정보 보호업무를 수행하는 담당부서에 관해서는 본 가이드북 제3장 개인정보 준법 구조의 제3.5절 기업의 의무 중 제2항 개인정보보호 책임자 지정 또는 기구 설립의 의무를 참조.

유의 사항
개인정보 보안사건의 발생 가능성을 낮추기 위해 모니터링 시스템 구축, 비상대책 수립, 조치 보고서/기록 작성 및 보관, 정기적인 훈련을 실시해야 한다.

바. 주요 인터넷 플랫폼의 준법 의무

「개인정보 보호법」 제58조에 따르면, 주요 인터넷 플랫폼 서비스를 제공하고 이용자 수가 매우 많으며 업무 유형이 복잡한 개인정보처리자의 경우, 다음의 의무를 이행해야 한다.

① 법령에 따라 온전한 개인정보보호 준법 시스템을 구축하고, 주로 외부인으로 구성된 독립기구를 설치하여 개인정보보호 상황을 감독해야 한다.
② 공개•공평•공정의 원칙에 따라 플랫폼 규칙을 제정함과 동시에 플랫폼상 제품이나 서비스 공급자의 개인정보 처리 기준과 개인정보보호의무를 명확히 해야 한다.
③ 플랫폼상의 제품이나 서비스 제공자가 법률 또는 행정법규를 중대하게 위반하는 경우, 즉시 관련 서비스 제공을 중단해야 한다.
④ 개인정보보호에 관한 사회적 책임 보고서를 정기적으로 발간하고 사회적으로 감독을 받아야 한다.

유의 사항
현재, 주요 인터넷 플랫폼 관련 진입(외상투자) 기준, 규범 및 특정 요구 사항에 관한 규정은 두고 있지 않으므로, 중국의 입법동향, 법령의 개정, 법집행 및 사법 사례에 주의를 기울여야 한다. 만약 기업이 주요 인터넷 플랫폼 사업자로 지정된 경우, 앞서 언급한 법적 요구 사항에 따라 개인정보보호 관련 의무를 이행해야 한다.

제 6절 개인정보의 국외 이전

가. 개인정보 국외 이전 시나리오

「개인정보 보호법」과 관련 법령에 따르면, 개인정보의 국외 이전은 다음과 같은 상황을 포함한다.

① 개인정보처리자가 개인정보를 직접 국외 서버로 이전하는 경우. 예를 들어, 기업이 베이징지점 고객의 개인정보를 서울 본사 서버로 이전하는 행위는 이에 해당한다.

② 개인정보처리자가 물리적 저장매체(예: USB 디스크)를 이용하여 개인정보를 국외의 이전 받는 자에게 전달하는 경우.

③ 국외의 주체가 중국 국내에 보관하고 있는 개인정보에 접근하는 경우. 예를 들어, 서울 본사 직원이 베이징지점 서버에 보관하고 있는 고객 개인정보에 원격으로 접근하는 경우.

④ 중국 국내에 소재하지만 중국의 사법관할이 아니거나 중국 국내에 등록되지 않은 주체에게 개인정보를 이전하는 경우. 예를 들어, 베이징에 등록된 한국 기업이 대한민국 대(영)사관으로 개인정보를 이전하는 행위는 이에 해당한다.

기업을 운영하는 과정에서 위의 상황이 발생하면 모두 개인정보의 국외 이전에 해당한다.

나. 개인정보의 국외 이전에 관한 기본 규칙

「개인정보 보호법」 제38조 ~ 제40조에서는 다양하고 적법한 국외 이전 경로를 규정하고 있으며, 개인정보의 국외 이전에 대한 일반적인 요구 사항뿐만 아니라 다양한 유형의 개인정보처리자에 대한 특정 요구 사항도 규정하고 있다.

<다양한 유형의 개인정보 처리자에 대한 요구사항>

일반 규칙	주체의 성격	특별 규칙
· 국외에서 개인정보를 이전 받는 자의 개인정보 처리가 「개인정보 보호법」에서 규정하는 개인정보보호 기준에 적합하도록	· 핵심정보인프라시설 운영자(Critical Information Infrastructure Operator: CIIO)의 경우 (개인정보 처리량이 국가네트워크정보 당국에서	· 중국 국내에서 수집 및 생성된 개인정보를 중국 국내에 보관해야 한다. · 국외 이전이 필요한 경우 국가네트워크정보 당국에서 주관하는 안전성 평가를 통과해야 한다.

필요한 조치를 취해야 한다. · 개인정보 주체에게 고지하고 별도의 동의를 얻어야 한다. · 사전에 미리 개인정보 보호 영향평가를 실시해야 한다.	정한 기준에 도달한 개인정보처리자)	
	· 기타 개인정보처리자의 경우	아래 조건 중 어느 하나에 해당하는 경우 국외 이전이 가능하다: · 국가네트워크정보 당국의 규정에 따라 전문 기관으로부터 개인정보보호 인증 실시 · 국가네트워크정보 당국에서 정한 표준계약에 따라 국외의 이전 받는 자와 계약을 체결하고 양자의 권리와 의무 약정 · 법령에 따른 기타 조건

① 개인정보처리자에 관한 일반 규칙

개인정보처리자가 중국 국외로 개인정보를 이전하는 경우, 다음의 세 가지 일반 규칙을 준수해야 한다.

·「개인정보 보호법」 제38조에 따르면, 개인정보처리자는 국외에서 개인정보를 이전 받는 자의 개인정보 처리가 「개인정보 보호법」에서 규정하는 개인정보보호기준에 적합하도록 필요한 조치를 취해야 한다.

·「개인정보 보호법」 제39조에 따르면, 개인정보처리자는 국외의 개인정보를 이전 받는 자의 명칭 또는 성명, 연락처, 처리목적, 처리방법, 개인정보의 종류 및 국외의 개인정보를 이전 받는 자를 대상으로 권리를 행사하는 방법과 절차 등을 개인정보 주체에게 고지하고 별도의 동의를 얻어야 한다.

·「개인정보 보호법」 제55조에 따르면, 개인정보처리자는 사전에 미리 개인정보 보호 영향평가를 실시하고 처리상황을 기록해야 한다

② “핵심정보인프라시설 운영자” 및 “개인정보 처리량이 국가네트워크정보 당국에서 정한 기준에 도달한 개인정보처리자”에 관한 특별 규칙

「개인정보 보호법」 제40조에 따르면, “핵심정보인프라시설 운영자” 및 “개인정보 처리량이 국가네트워크정보 당국에서 정한 기준에 도달한 개인정보처리자”는 중국 국외로 개인정보를 이전하는 경우, 앞서 언급한 세 가지 일반 규칙 외에 다음 규칙도 준수해야 한다.

· 중국 국내에서 수집 및 생성된 개인정보를 중국 국내에 보관해야 한다.

· 국가네트워크정보 당국에서 주관하는 안전성 평가에 통과해야 한다. 다만, 안전성 평가에 관한 구체적인 절차와 요구 사항은 향후 입법과 실천을 통해 확인 필요하므로, 기업으로서는 이에 대해 주의 깊게 살펴봐야 한다.

또한, "핵심정보인프라시설 운영자"에 관한 자세한 정의는 본 가이드북 제2장 「개인정보 보호법」 상 주요 정의 제2.11절 핵심정보인프라시설 운영자를 참조한다. "개인정보 처리량이 국가네트워크정보 당국에서 정한 기준에 도달한 개인정보처리자"에 관한 정의는 향후 네트워크정보 당국이 정하는 구체적인 법규를 통해 확인할 수 있을 것으로 예상한다.

③ 기타 개인정보처리자에 관한 특별 규칙

「개인정보 보호법」 제38조에 따르면, 핵심정보인프라시설 운영자 외의 기타 개인정보처리자가 중국 국외로 개인정보를 이전하는 경우, 앞서 언급한 일반 규칙 외에 다음 규칙 중 어느 하나를 충족해야 한다.

· 국가네트워크정보 당국에서 주관하는 안전성 평가에 통과
· 국가네트워크정보 당국의 규정에 따라 전문 기관으로부터 개인정보보호 인증 실시
· 국가네트워크정보 당국에서 정한 표준계약에 따라 국외의 이전 받는 자와 계약을 체결하고 양자의 권리와 의무 약정
· 법률, 행정법규 또는 국가네트워크정보 당국에서 정한 기타 조건

핵심정보인프라시설 운영자 외의 기타 일반 개인정보처리자는 「개인정보 보호법」에서 정하는 개인정보의 국외 이전에 관한 특별 규칙, 즉 상기 조건 중 어느 하나를 자유롭게 선택할 수 있다.

유의 사항
개인정보의 국외 이전에 대한 기본 규칙 및 요구 사항과 관련하여 다음 사항에 유의해야 한다. - 중국사업을 계획하거나 추진할 때 사전에 미리 개인정보의 국외 이전 이슈를 감안해야 함과 동시에, 자신이 해당하는 주체의 유형을 확인하여 실제 상황에 따라 국외 이전에 관한 준법 조치를 채택해야 한다. - 개인정보의 국외 이전 시나리오를 분석한 후 계약체결, 감사 및 평가, 기술적 모니터링 등 조치를 통해 국외에서 개인정보를 이전 받는 자도 동일한 보호수준을 유지하도록 해야 한다.

- 개인정보 주체에게 고지 및 별도의 동의를 받고 사전에 미리 개인정보보호 영향 평가를 실시하여 효과적인 보호조치를 취해야 한다.
- 현재까지 네트워크정보 당국에서 개인정보의 국외 이전에 관한 표준계약을 발표하지 않았으므로, 네트워크정보 당국의 통지나 동향을 주의 깊게 살펴보면서 개인정보의 국외 이전에 관한 사내 제도와 규범을 제때에 조정해야 한다.

다. 외국 사법 또는 법집행 기관의 중국 국내에 보관하고 있는 개인정보 조회 요청에 대한 대응

중국 대륙지역에서 사업을 영위하는 한국기업이 외국의 사법 또는 법집행 기관(예: 한국법원)으로부터 중국 국내에 보관하고 있는 개인정보에 대한 조회 요청을 받을 수도 있다. 이 경우, 기업은 「개인정보 보호법」 제41조에 따라 개인정보를 요구하는 사법 또는 법집행 기관이 소재하는 국가와 중국 정부 간에 개인정보의 국외 이전에 관한 국제조약을 체결했는지 여부를 먼저 확인해야 한다. 만약 관련 국제조약을 체결하였다면 해당 국제조약에 정해진 절차에 따라 중국 국내에 보관하고 있는 개인정보를 외국의 사법 또는 법집행 기관에 제출할 수 있다. 반대로, 관련 국제조약을 체결하지 않았다면 반드시 중국 대륙지역의 주관당국으로부터 허가를 받은 후에야 외국의 사법 또는 법집행 기관에 관련 개인정보를 제출할 수 있다.[21]

제 7절 감독기관과 기업 간의 협력

중국 행정당국의 감독시스템과 직책분담 상황을 감안하여 「개인정보 보호법」에서는 모든 분야의 개인정보보호와 감독직책을 하나의 부서로 통합하지 않고 있다.

가. 개인정보보호업무를 수행하는 담당부서 및 직권 구분

「개인정보 보호법」 제60조에 따르면, 개인정보보호업무를 수행하는 담당부서에는 국가네트워크정보 당국, 국무원 유관 부서, 현(縣) 단위 이상 지방정부 유관 부서가 포함된다.

① 국가네트워크정보 당국

21) 2022년 4월 현재, 한중간 협약이 체결되어 있지 않다.

현재 중국의 국가기관 구성상 국가네트워크정보 당국이란 “국가네트워크정보국(国家互联网信息办公室)”을 의미한다. 「개인정보 보호법」 제62조에 따라 국가네트워크정보 당국은 개인정보보호 업무와 관련 관리감독 업무를 총괄하여 책임지며 구체적으로 다음 사항을 포함한다. ① 개인정보보호에 관한 구체적인 규칙과 기준 제정. ② 소규모 개인정보처리자, 민감 개인정보 처리 및 안면인식, 인공지능 등 신기술, 새로운 응용에 대해서는 전문적인 개인정보 보호 규칙, 기준 제정. ③ 안전하고 편리한 전자 신원인증 기술의 연구개발과 보급 응용을 지원하고, 온라인 신원인증을 위한 공공서비스 구축 추진. ④ 개인정보보호를 위한 사회적 서비스 시스템 구축을 추진하고, 관련 기관의 개인정보보호 평가 및 인증 서비스 지원. ⑤ 개인정보보호 관련 불만사항 및 신고 업무 시스템 개선.

② 국무원 유관 부서

국무원 유관 부서에는 중국인민은행[22], 국가시장감독관리총국, 공업정보화부, 공안부, 교통운수부, 국가발전개혁위원회, 국가라디오방송총국 등을 포함하되 이에 국한되진 않는다. 국무원 유관 부서는 「개인정보 보호법」과 관련 법률, 행정법규에 의거하여 소관 범위 내에서 개인정보보호 및 관리감독 업무를 책임진다.

예를 들어, 「신용조사업 관리조례」 제7장의 규정에 따르면, 신용조사 과정에서의 개인정보 침해행위는 국무원의 신용조사감독관리 당국이나 그 파견기관에서 감독하고 조치한다. 따라서 중국인민은행은 신용조사 과정에서의 개인정보 침해행위에 대해 감독하고 조치할 권리를 갖는다.

③ 현(县) 단위 이상 지방정부 유관 부서

현(县) 단위 이상 지방정부 유관 부서란 현(县)•시(市)•성(省) 단위 지방정부의 유관 부서를 가리키며 현•시•성 단위의 시장감독관리국, 공안국(청), 교통운수국(청) 등을 포함하되 이에 국한되는 것은 아니다. 현 단위 이상 지방정부 유관 부서의 개인정보보호 및 관리감독 직책은 관련 국가규정에 따라 결정한다.

예를 들어, 「전기통신 및 인터넷 이용자 개인정보보호 규정」 제3조에 따르면, 공업정보화부와 각 성•자치구•직할시의 통신관리국은 법에 의거하여 전기통신

22) 중국인민은행은 중국의 중앙은행으로서 한국의 한국은행과 유사한 기능을 한다.

및 인터넷 이용자의 개인정보보호 업무에 대해 관리하고 감독한다. 따라서, 베이징시통신관리국은 베이징 시내 전기통신 및 인터넷 이용자의 개인정보보호 업무에 대해 관리하고 감독하는 권리를 갖는다. 「중국인민은행 소비자 권익 보호 실시 방법」 제5조에 따르면, 중국인민은행과 그 지점은 공평•공정 원칙에 따라 법에 의거하여 직책 범위 내에서 금융소비자의 이익을 보호하고 법적 권익을 보호해야 한다. 예를들어, 중국인민은행 상하이지점은 상하이 시내 소비자의 금융정보 보호 업무를 수행하는 권리를 갖는다.

나. 개인정보보호업무를 수행하는 담당부서[23]의 기본 직책 및 법 집행 조치

「개인정보 보호법」 제61조, 제65조에 따르면, 개인정보보호업무를 수행하는 담당부서의 기본 직책은 다음과 같다. ① 개인정보보호 홍보 및 교육을 실시하고 개인정보처리자의 개인정보보호 업무에 대해 지도 및 감독. ② 불만사항 및 신고 수리를 위한 연락처를 공개하고, 개인정보보호 관련 불만사항 및 신고를 처리하며, 처리 결과를 적시에 민원인 및 신고자에게 통지. ③ 애플리케이션 등의 개인정보 보호 상황에 대해 평가하고 결과를 공개. ④ 법을 위반한 개인정보 처리활동에 대해 조사, 처리. ⑤ 법률, 행정법규에서 규정한 기타 직책.

「개인정보 보호법」 제63조와 제64조에 따르면, 개인정보보호업무를 수행하는 담당부서가 취할 수 있는 법 집행 조치는 다음과 같다. ① 관련 당사자에 대한 질문을 통해 개인정보 처리활동 상황 조사. ② 개인정보 처리활동과 관련된 당사자의 계약서, 기록, 장부 및 기타 자료 열람, 복사. ③ 현장 조사를 통해 불법적인 개인정보 처리가 의심되는 행위에 대해 조사. ④ 개인정보 처리활동과 관련된 설비와 물품을 확인하여 불법적인 개인정보 처리활동에 이용되었음을 입증하는 증거가 있는 경우, 소속 부서의 주요 책임자에게 서면으로 보고한 후 승인에 따라 봉인 또는 압수. ⑤ 개인정보 처리활동에 비교적 큰 위험이 존재함을 발견하거나 개인정보 보안사건이 발생하는 경우, 개인정보처리자의 법인대표나 주요 책임자 대상으로 면담하거나, 개인정보처리자에게 전문 기관에 위탁하여 개인정보 처리활동에 대한 준법감사를 받을 것을 요구. ⑥ 불법적인 개인정보 처리가 범죄로 의심되는 경우, 즉시 공안기관에 송치하여 법에 의거하여 처리.

아울러, 「개인정보 보호법」 제63조에 따르면, 개인정보보호업무를 수행하는 담당부서가 법에 의거하여 직무를 이행할 때, 당사자는 이에 협조해야 하며 업무 집행을

23) 회사(개인정보처리자) 내의 부서(팀)을 의미하는 것이 아니라 법을 집행하는 정부기관을 의미한다.

거부하거나 방해해서는 안 된다. 따라서 기업은 개인정보보호 관리감독 부서가 직무를 수행할 때 관련 자료를 적극 제공하고, 유관 부서의 개인정보 보안 검사 업무에 협력하며, 관리감독 부서의 요구에 따라 적시에 시정해야 한다.

유의 사항
감독기관의 법 집행 조치와 관련하여 다음 사항에 유의해야 한다. - 기업이 속한 업종과 지역을 정확하게 파악하여 우선 관할 감독기관을 판단해야 한다. 그 후, 개인정보보호책임자(있는 경우) 또는 개인정보보호 분야에서의 업무 경험이 풍부한 책임자를 지정하여 감독기관과의 소통을 유지하면서 개인정보보호 및 사고처리 상황을 통보 또는 신고해야 한다. - 감독기관에서 발표하는 규칙, 지침 및 법 집행 동향에 대해 주의 깊게 살펴보아야 한다. 특히, 「개인정보 보호법」 제62조에서 최초로 “소규모 개인정보처리자”라는 개념을 언급[24]하였는바, 소규모 기업의 경우 소규모 개인정보처리자를 대상으로 하는 감독기관의 개인정보보호 규칙과 기준 제정 및 발표 동향에 대해 각별히 유의해야 하며, 관련 법령에 따라 개인정보 처리활동을 규범화해야 한다.

제 8절 책임 부담

「개인정보 보호법」 제66조~제71조에서는 개인정보처리자가 부담해야 하는 법률 책임(민사적, 행정적, 형사적 책임 포함)과 개인정보의 공익소송 제도에 대해 규정하고 있다.

가. 민사적 책임

「개인정보 보호법」에서는 개인정보의 권익침해에 대한 책임인정 원칙과 손해배상액 산정방법을 규정하고 있으며 자세한 내용은 다음과 같다.

① 과실책임의 추정: 「개인정보 보호법」 제69조 제1항에 따르면, 개인정보 처리로 인해 개인정보의 권익이 침해되었을 때 개인정보처리자는 자신의 과실이 없음을 입증할 수 없는 경우, 손해배상 등 침해 책임을 지도록 규정하고 있다. 즉, 「개인정보 보호법」은 개인정보가 침해당했을 시 손해배상 책임의 귀책원칙을 명확히 하고 있다.

② 배상액의 산정: 「개인정보 보호법」 제69조 제2항에 따르면, 개인정보 권익

24) 다만, “소규모 개인정보처리자”에 대한 구체적 정의는 담고 있지 않다.

침해에 따른 손해배상책임은 개인정보 주체가 입은 손해 또는 개인정보 처리자가 그로 인해 취득한 수익에 따라 산정된다. 만약 개인이 입은 손해와 개인정보처리자가 취득한 수익을 파악하기 어려운 경우 실제 개인정보 침해 상황에 따라 배상액을 정한다.

나. 행정적 책임

① 개인정보 처리 규정 위반에 따른 행정처벌 : 「개인정보 보호법」 제66조에 따르면, 개인정보처리자는 다음 두 가지 사항에 해당되는 경우에 행정처벌 될 수 있다. 첫째, 「개인정보 보호법」을 위반하여 개인정보를 처리하는 경우. 둘째, 개인정보를 처리하는 과정에 「개인정보 보호법」에 명시된 개인정보보호의무를 이행하지 않은 경우. 구체적인 책임은 다음과 같다.

- 일반적인 위법행위에 따른 행정처벌 : 「개인정보 보호법」 제66조 제1항에 따르면, 상기 위법행위가 일반적인 경우에 해당하는 경우, 개인정보보호 업무를 수행하는 담당부서는 다음과 같은 조치를 취할 수 있다.
  · 시정명령
  · 경고처분
  · 불법수익 몰수
  · 개인정보를 불법으로 처리한 애플리케이션에 대해 서비스를 일시 정지하거나 중단하도록 명령
  · 만약 시정하지 않을 경우, 개인정보처리자에 대해 100만 위안(한화 약 1억 8400만원) 이하의 과징금을 부과하고, 직접 책임이 있는 주요 관리자와 기타 담당자에 대해서는 1만 위안(한화 약 184만원) 이상 10만 위안(한화 약 1,840만원) 이하의 과징금을 부과.
- 중대한 위법행위에 따른 행정처벌 : 「개인정보 보호법」 제66조 제2항에 의거, 상기 위법행위가 중대한 경우에 해당하는 경우, 성(省) 단위 이상의 개인정보 보호업무를 수행하는 담당부서는 다음과 같은 조치를 취할 수 있다.
  · 시정명령
  · 불법수익 몰수
  · 아울러, 5,000만 위안(한화 약 92억원) 이하 또는 전년도 매출액의 5% 이하에 해당하는 과징금을 부과. 또한 관련 업무의 일시 정지 명령, 시정을 위한 영업중단 명령, 관련 주관부서에 영업허가 또는 사업자등록증 취소 통보

명령을 내릴 수 있음.

· 직접 책임을 부담하는 주요 관리자와 기타 직접 담당자에 대해서는 10만 위안(한화 약 1,840만원) 이상 100만 위안(한화 약 1억8400만원) 이하의 과징금에 처하고, 일정기간 동안 해당 기업의 이사, 감사, 임원 및 개인정보보호책임자로 활동하는 것을 금지할 수 있음

또한, 「개인정보 보호법」 제71조에 따르면, 개인정보처리자가 「개인정보 보호법」을 위반하여 치안관리 위반 행위를 한 경우, 유관 부서는 「치안관리처벌법」 및 기타 관련 법령에 따라 처벌 할 수 있다.

② 「개인정보 보호법」 위반 시 신용보고서 기록 및 공시에 관한 행정처벌

「개인정보 보호법」 제67조에 따르면, 「개인정보 보호법」위반시, 관련 법률 및 행정법규에 의거하여 개인 또는 기관의 신용보고서에 위법행위를 기록하고 공시한다.

③ 개인정보보호의무를 이행하지 않는 국가기관의 책임

「개인정보 보호법」 제68조에 따르면, 국가기관이 「개인정보 보호법」에 규정된 개인정보보호의무를 이행하지 않은 경우, 그 상급기관 또는 개인정보보호업무를 수행하는 담당부서에서 시정 명령하고, 직접 책임을 부담하는 주요 관리자와 기타 직접 담당자에 대해 법적 처벌한다. 또한, 개인정보보호업무를 수행하는 부서의 담당자가 업무상 직무유기, 직권남용 또는 부정행위를 저질렀을 경우 범죄가 되지 않을지라도 법에 따라 처벌한다.

다. 형사책임

「개인정보 보호법」 제71조에 따르면, 「개인정보 보호법」을 위반하여 범죄를 구성하는 경우 형사 책임을 진다. 동 조항은 「형법」 제253조의1 국민의 개인정보 침해에 따른 범죄 및 형벌과 관련되며 자세한 내용은 다음과 같다.

① 개인정보처리자가 개인정보를 타인에게 판매하거나 제공하는 행위로 인해 국가 규정을 위반하고 그 사정이 중대한 경우, 3년 이하의 유기징역 또는 구역(拘役, 형기가 비교적 짧은 징역형)과 함께 벌금을 병과(併科)하거나 단순 벌금에 처한다. 단, 특별히 중대한 사안의 경우, 3년 이상 7년 이하의 유기징역과 함께 벌금을 병과한다.

② 개인정보처리자가 직무를 수행하거나 서비스를 제공하는 과정에서 취득한 국민의 개인정보를 국가 규정을 위반하고 타인에게 판매 또는 제공하는 경우 ①항의 규정에 따라 중벌에 처한다.

③ 단체 또는 개인이 국민의 개인정보를 절취하거나 기타 불법적인 방법으로 취득한 경우,①항의 규정에 따라 처벌한다.

④ 단체가 전 3항의 범죄를 구성하는 경우 벌금에 처함과 동시에, 직접 개인정보보호 업무를 책임지는 주요 관리자와 기타 직접 담당자에 대해서도 상기 규정에 따라 처벌한다.

라. 공익소송에 관한 특례

「개인정보 보호법」 제70조에서는 개인정보에 관한 공익소송제도에 대해서도 규정하고 있다. “공익소송”이란 사회적 공공이익을 목적으로 특정기관, 사회단체 또는 개인이 제기하는 소송 행위를 의미한다.

「개인정보 보호법」 제70조에 따르면, 개인정보처리자가 「개인정보 보호법」을 위반하여 개인정보를 처리함으로 인해 다수 개인의 권익이 침해된 경우, 인민검찰원, 법에서 정한 소비자조직 및 국가네트워크정보 당국에서 지정한 조직은 법에 의거하여 인민법원에 소송을 제기할 수 있다. 단, 그 중 “국가네트워크정보 당국에서 지정한 조직”에 해당하는 요건은 현재 명확하지 않다.

유의 사항
책임과 관련하여 다음 사항에 유의해야 한다. - 기업이 준법업무를 수행할 때 관련 제도, 일지, 평가보고서 및 기타 서류 보관에 주의를 기울여야 한다. 이러한 서류는 관련 분쟁 발생 시 증거로 사용될 수 있다. - 개인정보보호를 위한 준법 시스템의 구축을 강화하고, 임직원들의 개인정보보호 의식을 향상시키며, 개인정보를 침해하고 개인정보 주체의 권익을 침해하는 사고를 예방해야 한다.

제 4장 업무 유형별 개인정보보호 대응 방법

「개인정보 보호법」이 시행된 후, 개인정보 준법감시에 있어 각 산업별로 모두 커다란 도전에 마주치게 되었다. 따라서 본 가이드북에서는 기업이 참고할 수 있도록 몇가지 시나리오와 업종을 예로 들어 소개한다.

제 1절 웹사이트 및 애플리케이션(APP) 운영 시나리오

웹사이트 또는 애플리케이션(App)을 운영하는 기업이 특히 주의해야할 사항은 다음과 같다.

가. 상황인지 동의

기업이 웹사이트 또는 애플리케이션(App)을 운영할 때 "상황인지 동의(informed consent)"는 개인정보를 처리하는 중요한 법적 근거다. 더불어, 「개인정보 보호법」에서도 개인정보처리자가 합리적인 조치를 취해 개인정보 주체가 상황을 인지하는 전제 하에 동의하도록 규정하고 있다. 개인정보주체가 상황을 인지하는 것은 개인정보처리자의 설명의무와도 관련이 있다. 예를 들어, 「개인정보 보호법」 제17조 제3항에서는 개인정보처리자가 개인정보 주체의 열람과 보관을 용이하게 하기 위해 처리 규정을 공개하도록 규정하고 있다. 따라서 기업은 웹사이트 또는 애플리케이션(App)을 운영할 때 이용자가 관련 처리 규정을 조회할 수 있도록 특정 웹 페이지를 설정하는 동시에 다운로드 경로를 제공해야 한다. 또한, 「애플리케이션(APP)에 의한 개인정보 무단 수집 및 이용 행위 판정 방법」에서도 "상황인지 동의"에 관해 규정하고 있으며 자세한 내용은 다음 세 가지를 포함한다. (1) 최초 실행 시, 팝업창 등의 명확한 방식을 통해 이용자가 「개인정보보호정책」을 읽어보도록 안내해야 한다. (2) "4번의 클릭" 이내에 개인정보 처리 규정에 접근할 수 있도록 해야 한다. (3)「개인정보보호정책」은 중국어로 작성해야 하며 이해하기 쉽고 읽기 편해야 한다.

유의 사항
기업이 웹사이트 또는 애플리케이션(App)을 운영하는 경우, 「개인정보보호정책」 또는 「개인정보보호방침」에 다음 내용을 포함시킬 것을 권장한다. - 웹사이트 또는 애플리케이션(App) 사업자 명칭 및 연락처 - 개인정보의 종류, 처리목적, 처리방법 및 보관기간 - 「개인정보 보호법」에 따른 개인정보 주체의 권리행사 방법 및 절차

- 개인정보보호책임자 연락처(기업의 개인정보 처리량이 법적 기준에 도달한 경우)
- 법에 의해 공개해야 하는 기타 내용

나. 정당한 권리 취득을 위한 구체적인 방법

「개인정보 보호법」 제5조에서는 개인정보 처리에 관한 정당성 원칙을 규정하고 있다. 웹사이트 및 애플리케이션(App) 분야에 있어, 개인정보처리 행위가 「개인정보 보호법」 제5조의 정당성 원칙을 충족시키기 위해, 「애플리케이션(APP)에 의한 개인정보 무단 수집 및 이용 행위 판정 방법」과 「모바일 인터넷 앱 개인정보보호 관리 잠정 규정(의견수렴안)」을 참고할 것을 권장한다.

유의 사항
기업이 웹사이트 또는 애플리케이션(App)을 이용하여 고객정보를 수집하고 처리하는 경우, 다음 사항에 유의해야 한다. - 개인정보 처리 권한을 이용하기 전에 개인정보 주체에게 해당 권한에 대한 목적을 명확하게 고지해야 한다. - 개인정보 주체가 동의하기 전까지 기업의 웹사이트나 애플리케이션(App)은 개인정보에 접근할 수 없다. - 개인정보 주체가 개인정보 처리 행위에 동의하지 않을 경우, 기업의 웹사이트 및 애플리케이션(App)은 반복적으로(지속적, 빈번하게) 개인정보 주체의 동의를 구해서는 아니 된다. - 개인정보 수집 및 이용의 진실된 목적이나 처리범위를 고의로 기만하거나 은폐하여 개인정보 주체로부터 권한을 취득해서는 아니 된다. - 웹사이트 및 애플리케이션(App)의 동의 표시 박스나 경로에 묵시적으로 동의가 표시되어 있어서는 안 된다. - 기업의 웹사이트 및 애플리케이션(App)은 버전 업데이트 후, 이용자가 설정한 개인정보 권리승인 상태를 자동으로 조정할 수 없다. - 개인정보 주체에게 반드시 한 번에 여러 시스템을 열어 권한을 부여하도록 요구할 수 없으며, 관련 권한을 부여하도록 강요할 수도 없다.

다. 필요한 최소 범위의 명확 원칙

기업은 웹사이트 또는 애플(APP)을 운영함에 있어 「개인정보 보호법」에서 규정하고 있는 필요한 최소 범위의 원칙을 준수해야 하며, 개인정보의 처리목적, 처리방법, 수집범위 및 보관기간 4가지 모두 적용해야 한다. 기업은 가능한 신속하게 개인정보에 관한 처리목적, 처리방법, 수집범위 및 보관기간을 명확히 해야 한다.

유의 사항
- 「모바일 인터넷 애플리케이션(App) 개인정보보호 관리 잠정 규정(의견수렴안)」 제7조는 애플리케이션(App) 사업자에 대해 “개인정보 처리의 수량, 빈도 및 정확성이 서비스에 반드시 필요한 것인지”에 대해 검토해야 한다고 명시하고 있으므로, 기업은 상기 요건을 충족하기 위해 정기적인 검토 시스템을 마련해야 한다. - 업종 및 기업마다 처리해야 하는 최소한의 개인정보의 범위가 다를 수 있으므로, 2021년 3월에 고시된 「일반 유형의 모바일 인터넷 애플리케이션(App)에 필요한 개인정보 범위에 관한 규정」을 참고할 수 있다. 위 규정은 39가지 애플리케이션(App)의 기본 기능과 필요한 개인정보의 범위를 규정하고 있으므로, 기업은 자체 상황에 따라 처리해야 하는 최소한의 개인정보 범위를 정할 수 있다.

라. 민감 개인정보의 특별 처리

기업이 운영하는 웹사이트 또는 애플리케이션(App)이 민감 개인정보를 포함하는 경우, 「개인정보 보호법」 제28조~제31조에 따라 특별 처리해야 한다. 기업이 운영하는 웹사이트 또는 애플리케이션(App)이 민감 개인정보 처리를 포함하는 경우, 다음 사항에 유의할 필요가 있다.

첫째, 만 14세 미만 미성년자의 개인정보를 처리하는 경우. 이 규정이 게임류와 SNS류의 웹사이트 및 애플리케이션(App)에 큰 영향을 미칠 것으로 예상된다. 이에 해당하는 기업은 「개인정보 보호법」의 규정에 따라 별도의 미성년자 개인정보 처리 시스템을 마련하여 미성년자의 개인정보를 별도로 처리해야 한다.

둘째, 개인정보 주체의 위치정보 처리. 「개인정보 보호법」이 제정되기 전 많은 웹사이트나 애플리케이션(App)에서 위험관리를 목적으로 개인정보 주체의 위치정보를 수집하여 위법행위(예: 전자상거래시 허위판매 등) 여부를 판단하였다. 그러나 「개인정보 보호법」이 발효 후, 웹사이트나 애플리케이션(App)에서 수시로 개인정보 주체의 위치정보를 수집하는 행위가 민감 개인정보의 특정 목적과 충분한 필요성 요건을 충족하는지 여부에 대해서는 여전히 기업의 실제 경영상황과 향후의 법 집행 사례를 토대로 확인해야 할 필요가 있다.

셋째, 개인정보 주체에 대한 안면인식 기술 적용. 기업의 웹사이트 및 애플리케이션(App)은 안면인식 기술을 기반으로 이용자의 신원을 식별하거나 인증하는 경우가 있는데, 이 기술의 적용은 민감 개인정보 수집에 해당한다. 기업은 별도의 약정(민감 개인정보 처리의 충분한 필요성과 안면인식 거부 시 미치는 영향 명시)을 마련하고, 적법한 경우에만 이용자에게 안면인식 알림을 제공하여 개인정보 주체로부터 별도의 동의를 얻을 것을 권장한다.

마. 이용자의 권리 실현 시스템

「개인정보 보호법」은 개인정보 주체의 권익을 보호하기 위한 메커니즘을 규정하고 있으므로, 기업은 「개인정보 보호법」의 규정에 따라 웹사이트와 애플리케이션(App)을 적절하게 정비해야 한다.

유의 사항
다음과 같은 내용을 검토하고 정비할 것을 권장한다. - 개인정보 주체가 웹사이트나 App의 개인정보 처리 목적과 범위를 이해할 수 있도록 App이 “조회” 기능을 구현했는지 여부 - 개인정보 주체가 언제든지 개인정보 사본을 취득할 수 있도록 App이 “복사” 기능을 구현했는지 여부 - 개인정보 주체가 언제든지 개인정보를 정정 및 보완할 수 있도록 App이 “수정” 기능을 구현했는지 여부 - 개인정보 주체가 스스로 권한을 차단하거나 개인정보의 처리 범위를 축소 및 제한할 수 있도록 App이 “동의철회” 기능을 구현했는지 여부 - App이 “개인정보삭제” 기능(예: 계정해지 기능과 계정해지시 개인정보를 삭제하는 기능)을 구현했는지 여부 - App에 “자동화 의사결정”(예: cookies, 개인화된 추천 등) 기능이 있는지 여부와 자동화 의사결정에 따른 권한취득이 「개인정보 보호법」을 준수하는지 여부

바. 제3자 코드의 묵시적 삽입

기업이 웹사이트나 App에 SDK(Software Development Kit)를 삽입하고자 하는 경우, 「개인정보 보호법」에 따라 개인정보 주체에게 SDK의 사용 상황과 개인정보 처리의 목적, 범위, 방법 등을 미리 고지해야 한다. 아울러, 개인정보 주체가 상황을 인지한 후 본인 의사에 따라 기업의 웹사이트나 App이 SDK를 통해 개인정보를 처리할 수 있도록 권한을 부여할 것인지 여부를 결정할 수 있다.

유의 사항
웹사이트나 App에 대해 다음 조치를 취할 것을 권장한다. - 자사 SDK, 휴대전화 제조업체 SDK, 제3자 SDK 등을 포함하여 이미 웹사이트나 App에 연결된 모든 SDK에 대해 검토할 것 - 연결된 SDK 서비스 제공자와 충분한 소통과 함께, 기술평가 기관에 의한 기술적 검토 또는 SDK 서비스 제공자가 공시한 서비스 이용약관, 「개인정보보호정책」 등 관련 문서를 통해 웹사이트나 App에 연결된 SDK의 개인정보 처리 목적, 방법 및 범위에 대해 충분히 이해할 것 - 연결된 SDK의 개인정보 처리 목적, 방법 및 범위 등을 「개인정보보호정책」에

명시하고, 개인정보 주체로부터 개인정보 처리에 대한 동의를 얻을 것
- SDK를 통해 외부에 정보를 제공하거나 SDK 서비스 제공자에게 개인정보를 제공하는 경우, 개인정보 주체에게 해당 개인정보를 외부에 제공한다는 사실을 고지할 것
- 협약 및 기술적 수단을 통해 SDK에 대한 감독과 통제를 강화하여 SDK의 개인정보 처리 상황과 동향을 최대한 파악할 것
- 웹사이트나 App에 대한 업계 규제 동향에 주의를 기울이고, 새로운 정책이나 업계 사례가 나타날 경우 자체 상황에 따라 시정 또는 정비할 것

법률 안내

기업이 웹사이트나 App을 운영할 때 「개인정보 보호법」의 관련 규정을 준수하는 것 외에도 다음 규정과 표준을 함께 참고할 것을 권장한다.
- 「개인정보안전규범」(「GB/T 35273-20200 정보보안기술 - 개인정보 보안 규범」)
- 「일반 유형의 모바일 인터넷 앱에 필요한 개인정보 범위에 관한 규정」
- 「APP에 의한 개인정보 무단 수집 및 이용에 대한 자가진단 지침」
- 「APP에 의한 개인정보 무단 수집 및 이용 행위 판정 방법」
- 「사이버 보안 표준 실무 지침 - 모바일 인터넷 앱(App) 개인정보 수집 및 이용 자가진단 가이드라인」
- 「사이버 보안 표준 실무 지침 - 모바일 인터넷 앱(App)의 소프트웨어 개발 키트(SDK) 사용 관련 보안 가이드라인」
- 「모바일 인터넷 앱 개인정보보호 관리 잠정 규정(의견수렴안)」

제 2절 마케팅 과정에서의 개인정보 처리

기업은 마케팅 과정에서 자체 인지도를 높여 보다 많은 관심을 끌기 위해 종종 개인정보 주체에게 광고 등 마케팅 정보를 제공한다. 그러나 「개인정보 보호법」은 기업의 마케팅 행위에 커다란 영향을 미치게 되므로, 개인화된 추천(맞춤형 추천)과 광고 푸시(Push) 두 가지 주요 시나리오를 예로 들어 설명한다.

가. 개인화된 추천(맞춤형 추천)

① 개인화된 추천의 기준

“개인화된 추천”이란 특정 자동화 및 비자동화 기술을 이용하여 개인정보 주체의 특성을 분석하고 그에 대한 태그와 프로파일을 형성하는 것을 의미한다. 예를 들어, 개인정보 주체의 쇼핑 취향, 취미, 소비수준 등에 따라 태그 또는 프로파일을 분석하고, 그 결과에 따라 개인정보 주체별로 각기 다른 맞춤형 제품 및/또는 서비스를 푸시하거나 노출하는 행위가 이에 해당한다. 마케팅 시나리오에 있어 개인화된 추천은 일반적으로 많은 양의 개인정보를 처리해야 하므로 개인정보 처리에 관한 준법 요건을 충족해야 한다는 점에 유의하기 바란다. 개인화된 추천 적용 시나리오에서 개인정보 수집 및 이용에 관한 준법 요건을 충족함에 있어 다음 세 가지에 유의해야 한다.

i) 개인정보 수집 및 이용에 관한 일반 요구 사항을 충족해야 한다.
즉, 기업이 개인화된 추천 서비스를 할 때 「개인정보 보호법」에 명시된 개인정보 처리 원칙과 일반 처리 규칙 및 의무를 준수해야 한다. 또한, 기업은 「인터넷 개인정보보안 보호 지침」 제6.3 c)항에 따라 완전히 자동화 의사결정에 의존하는 이용자 프로파일 기술을 정밀 타겟 마케팅, 검색결과 순위 배정, 개인화된 뉴스, 타겟 광고 등 부가 서비스에 적용하는 경우, 사전에 이용자로부터 명시적인 권한을 얻지 않아도 되지만 이용자의 반대 또는 거절 권리는 보장해야 하는 점에 유의해야 한다.

ii) 개인화된 추천 목적에 따른 개인정보 수집 및 이용에 대한 요구 사항을 충족해야 한다.

「개인정보안전규범」 제7.5조에 따르면, 개인정보 주체에게 서비스 기능을 제공할 때 개인화된 노출 콘텐츠와 비개인화된 노출 콘텐츠를 명확하게 구분해야 한다.

나아가 구분할 때 “타겟 푸시(Push)” 등 문구를 명시하거나 다양한 카테고리, 섹션 및 페이지 등을 통한 별도의 노출 방법을 채택할 수 있으며 이에 국한하지는 않는다. 또한, 업종별로 개인화된 추천에 대한 특별한 요구 사항이 있을 수 있으며, 기업은 실제 상황에 따라 적용하거나 조정해야 한다.

iii) 특정 유형의 개인정보(예: 민감 개인정보, 개인금융정보) 처리에 대한 특별 준법 요건과 특정 산업의 규제 요건을 충족해야 한다.

민감 개인정보의 처리에 관해서는 본 가이드북 제3장 개인정보 준법 구조 제3.4절 개인정보 처리 규칙 제3항 개인정보 처리에 관한 특별규정 (8)민감 개인정보의 처리에서 이미 소개하였으므로, 거기서 언급된 유의 사항에 따라 자체적으로 검토하여 만약 특정 유형의 개인정보 처리 준법 요건을 위반한 경우에는 지체 없이 시정해야 한다.

② 이용자 프로파일링 및 자동화 의사결정

i) 이용자 프로파일링

“이용자 프로파일링”이란 개인정보를 수집, 취합 및 분석하여 직업, 경제상황, 건강, 교육, 개인취향, 신용, 행위 등과 같은 특정 자연인의 개인적 특성을 분석 또는 예측하여 개인적인 특징모델을 생성하는 과정을 의미한다. 직접적으로 특정 자연인의 개인정보를 이용하여 해당 자연인의 특징모델을 생성하는 것을 “직접 이용자 프로파일링”이라 한다. 반면, 특정 자연인 이외의 개인정보로부터 발생한 정보, 예를 들어 해당 자연인이 속한 그룹의 데이터를 이용하여 자연인의 특징모델을 생성하는 것을 “간접 이용자 프로파일링”이라 한다.

개인화된 추천은 이용자 프로파일링의 일반적인 적용 시나리오 중 하나로, 「개인정보 보호법」에서 이용자 프로파일링에 대해 직접적으로 규정하고 있지는 않지만 「개인정보안전규범」 제7.4조에서 다음과 같이 이용자 프로파일의 사용을 금지 또는 제한하고 있다.

첫째: 개인정보 주체의 특징 설명은 차별적이거나 모욕적인 내용을 금지한다. 다시 말해, 이용자 프로파일의 개인정보 주체 특징 설명 중 다음 내용을 포함할 수 없다.

(ㄱ) 외설, 음란, 도박, 미신, 테러, 폭력

(ㄴ) 민족, 인종, 종교, 장애, 질병 등에 대한 차별적인 표현

둘째: 이용자 프로파일 이용 목적 및 시나리오를 제한해야 한다. 즉, 기업이 사업 영위 또는 대외 업무협력 과정에서 이용자 프로파일을 사용할 때 다음과 같은 행위가 발생하지 말아야 한다.

(ㄱ) 국민, 법인 및 기타 단체의 적법한 권익 침해행위

(ㄴ) 국가안보, 명예 및 이익침해, 국가정권 전복선동, 사회주의체제 전복, 국가분열 선동 및 국가통일 파괴, 테러리즘 및 극단주의 조장, 민족증오 및 민족차별 고취, 폭력 및 음란외설적 정보 유포, 허위정보 날조•유포로 사회경제 질서 교란

(ㄷ) 개인정보를 사용할 때 개인정보 주체가 동의한 사용 목적을 달성하기 위해 필요한 것 외에, 특정 개인을 특정 지을 수 없도록 신원을 향한 지향성을 제거해야 한다.

또한, 기업이 생성한 태그와 이용자 프로파일을 이용하여 단독으로 또는 기타 정보와 결합하여 특정 자연인의 신원을 식별할 수 있거나 활동 상황을 반영할 수 있는 경우, 해당 태그와 프로파일은 개인정보에 해당하며 적절한 개인정보보호조치를 취해야 하는 점에 주의해야 한다.

ii) 자동화 의사결정

기업이 마케팅 수행 시 자동화 의사결정 방식을 채택하는 경우, 「개인정보보호법」 제24조의 자동화 의사결정 관련 규정을 준수해야 하며, 자세한 설명은 본 가이드북 제3장(개인정보 준법 구조) 제 4절(개인정보 처리 규칙)의 제3항 개인정보 처리에 관한 특별규정을 참고한다.

유의 사항
개인화된 추천을 이용하여 마케팅 수행 시, 다음 사항에 유의해야 한다. - 개인정보 주체에게 개인화된 추천 시나리오를 상세하게 알려 투명성을 보장해야 한다. - 개인화된 추천에 대한 자율적인 제어 메커니즘과 개인화된 노출에 대한 관리 방법을 구축하고, 「개인정보보호정책」 등의 방식을 통해 관련 메커니즘 및 관리 방법의 구현 경로를 고지해야 한다. - 별도의 개인화된 추천 섹션을 설정하여 추천 형식과 추천 시 의존하는 개인정보에 대해 구체적으로 명시하고, 자체 설정을 통해 추천을 스스로 해제하는 방법을 설명할 수 있다. - 개인정보처리자가 개인화된 추천 기능을 활성화했는지 여부와 관계없이 반드시 개인화되지 않은 추천 옵션 콘텐츠를 제공해야 한다. - 기업이 한 번의 추천으로 개인화된 추천과 개인화되지 않은 추천 콘텐츠를 동시에 제공할 수 없는 경우, 개인화된 추천과 개인화되지 않은 추천을 교차함으로써 개인화된 추천 콘텐츠만 제공하지 않도록 할 수 있다.

- 개인정보 주체가 개인화된 추천을 해제하면, 기업은 즉시 관련 개인정보 처리활동을 중단하고 지체 없이 관련 개인정보를 삭제하거나 익명화 처리해야 한다.

나. 광고 푸시

① 광고 푸시 기준

기업이 광고 푸시를 목적으로 개인정보를 수집하는 경우, 「개인정보 보호법」 및 관련 법령을 준수해야 한다. 해당 시나리오에 있어, 기업이 광고를 푸시할 때 아래 예시와 같은 개인정보보호 기준에 주의할 것을 권장한다.

- 기업이 광고를 푸시하는 과정에서 개인정보를 처리하는 행위는 필요한 최소 범위의 원칙을 준수해야 한다. 기업은 수집한 개인정보를 이용하여 개인화된 추천 방식으로 광고를 푸시하는 경우, 광고 푸시와 연관되는 개인정보만 개인화된 추천에 이용할 수 있다는 점에 유의해야 한다. 예를 들어, 휴대폰 대화 내용, 이용자 이미지 등의 정보를 광고 푸시에 이용하는 행위는 명백히 필요한 최소 범위의 원칙에 위배될 뿐만 아니라 상기 수집 및 이용 목적에도 적합하지 않으므로 해당 행위는 원칙적으로 금지되어야 한다.
- 기업이 개인화된 추천 방식으로 광고를 푸시하는 경우, 「개인정보 보호법」 및 관련 법률, 규정, 기준을 준수해야 한다. 또한, 기업이 다음 사항에 주의할 것을 권장한다. 첫째, 이용자가 개인화된 추천 방식의 광고 푸시를 선택하고 기업이 한 번에 하나의 광고만 푸시하는 경우, 개인화된 추천과 개인화되지 않은 방식의 광고를 교차하여 추천할 수 있다. 둘째, 기업이 개인화된 추천 방식의 광고를 푸시하는 경우, 푸시 기능을 해제할 수 있는 옵션이나 버튼을 제공하여 이용자가 언제든지 개인화된 추천 광고 모드를 해제할 수 있도록 해야 한다.

유의 사항
실제 운영 시, 개인정보의 수집 및 이용에 관한 규정을 준수하는 것 외에, 이용자에게 기업의 준법상황을 명확하게 알리고 이용자의 의심을 해소하기 위해 다음과 같은 방법을 취할 수도 있다. - 「개인정보보호정책」에 광고를 위해 수집 및 이용하는 개인정보의 종류를 열거하고 분석방법을 설명하는 동시에 관련 기능과 매칭시킬 수 있다. - 개인화된 추천 광고를 표시할 때 추천 메커니즘에 대한 이해를 높이고 오해를 해소하기 위해, 추천 원인(자동화 의사결정, 이용자 프로파일 생성 등 의사결정 알고리즘)을 간단하게 설명하거나, “**에 의한 추천” 등의 방식으로 추천 동기를 알리거나, 또는 관련 이용자 태그를 노출할 수 있다.

② 광고 분석 데이터

기업이 프로그래매틱 광고 모델[25]을 통해 이용자에게 광고를 푸시하는 경우, 광고 효과를 분석하기 위해 광고노출, 이용자 클릭, 구매 등의 정보 수집 시 다음 사항에 유의해야 한다.

- 개인정보의 판단: 먼저 프로그래매틱 광고 시나리오에 개인정보가 포함되는지를 판단해야 한다. 예를 들어, 이용자의 클릭 및 구매 행위 데이터에서 기업이 수집한 클릭 및 구매 횟수를 특정 개인과 연계시킬 수 없는 경우 개인정보에 해당하지 않는다. 그러나 기업이 수집한 데이터로 특정 이용자를 식별할 수 있는 경우라면 개인정보에 해당하므로 「개인정보 보호법」을 준수해야 한다.
- 개인정보 수집 방지: 광고 효과를 평가하는 시나리오에 있어, 때로는 개인을 식별할 수 있는 개인정보를 취득하지 않고도 필요한 분석을 달성할 수 있다는 점을 이해한다. 따라서, 이와 같은 시나리오에서 기업은 되도록 개인정보에 해당하는 데이터를 수집하는 것을 삼가야 한다. 만약 개인정보 수집이 필요한 경우라면, 수집 후 즉시 익명화 처리하거나 비식별화 처리한 다음 분석 및 활용할 것을 권장한다.
- 개인정보의 공유: 기업이 상기 개인정보를 제3자와 공유해야 하는 경우 비식별화 처리한 개인정보를 공유할 것을 권장하며, 아울러 해당 개인정보를 이전 받는 자가 개인정보 주체를 재식별하거나 연계시킬 수 없도록 보장해야 한다.

법률 안내
기업이 마케팅을 할 때 「개인정보 보호법」 준수와 함께 다음의 법규와 표준도 함께 참고할 것을 권장한다. - 「인터넷 광고 관리 잠정 조치」 - 「네트워크 거래 관리감독 방법」 - 「개인정보안전규범」 - 「인터넷 개인정보보안 보호 지침」

25) “프로그래매틱 광고” 모델은 자동화 시스템(또는 기술)과 데이터를 기반으로 기업의 광고노출 요청을 수행하는 인터넷 광고 거래 모델이다.

제 3절 사물인터넷 운영 시나리오

가. 사물인터넷 소개

사물인터넷은 인터넷과 같은 네트워크 시스템을 통해 감지노드 장치들을 연결하여 응용시스템을 구성한 것으로, 기본적으로 감지계층, 네트워크 계층 및 응용계층으로 구성된다. 사물인터넷은 일반 사물의 장치화, 자율 단말 상호연결, 범용 서비스 지능화 등 세 가지 특징을 갖는다. 사물인터넷은 비교적 넓은 개념이므로 특정 산업과 연계하여 다양한 네트워킹 시스템을 파생시킬 수 있다. 본 가이드북 제4장 업무 유형별 개인정보보호 대응 방법 제4.4절 차량인터넷 운영 시나리오에서 소개하는 차량인터넷 시나리오는 사물인터넷과 자동차 산업을 결합한 산물이다.

나. 사물인터넷 각 계층이 개인정보 처리에 미치는 위험 및 그에 대한 대응

① 감지계층 위험

사물인터넷 시나리오에서 기업은 감지계층의 다양한 감지단말, 센서, 스마트 장치, RFID 등을 이용하여 개인정보를 수집하는 데, 산업별 개인정보 수집 시나리오에 따라 수집되는 개인정보는 기본정보, 금융정보, 생체정보, 지리적 이동 위치정보 등을 포함하되 이에 국한되지 않는다.

사물인터넷을 통해 개인정보를 수집하는 경우, 주로 다음과 같은 두 가지 유형의 위험이 존재한다.

i) 개인정보 주체가 인지하지 못한 상황에서 개인정보 수집(즉, 인지하지 못한 상황에서의 수집). 인지하지 못한 상황에서의 수집은 개인정보 주체의 개인정보가 자동적으로 수집되는 것을 의미한다.

ii) 개인정보의 과도한 수집. 사물인터넷 시스템은 개인정보를 수집할 때 특정 개인정보만 골라서 수집하는 것이 아니라 불필요한 많은 양의 정보를 함께 수집할 수 있으므로, 개인정보가 급증하면서 위험부담이 커질 수 있다.

이때, 개인정보 주체가 인지하지 못한 상황에서의 수집과 무분별한 수집을 방지하기 위해 「개인정보 보호법」 및 관련 법령, 표준에 따라 사물인터넷 시스템을 업데이트해야 한다.

또한, 「GB/T 37024-2018 정보보안기술 - 사물인터넷 감지계층 게이트웨이 보안기술 요구 사항」 제6.2조에 따라 기업이 사물인터넷 감지계층에 개인정보를

저장해야 하는 경우, 감지계층 게이트웨이에 의해 저장되는 개인정보의 무결성에 대한 모니터링 메커니즘이 마련되어야 하며, 아울러 식별정보, 프로토콜 변환 규칙, 감사 기록 등의 중요한 개인정보에 대한 무결성 모니터링을 구현해야 한다.

② 네트워크 계층 위험

네트워크 계층에서의 가장 큰 위험은 지역을 넘나드는 개인정보의 전송과 저장에서 비롯한다. 또한, 사물인터넷 감지단말의 방어력이 취약하기 때문에 이러한 단말들이 공격자에 의해 악용되어 핵심 네트워크 시스템을 차단하거나 서비스를 중단시킬 수 있다. 개인정보가 사물인터넷 내에서 전송될 때 위와 같은 상황이 발생하면, 개인정보가 유출되어 개인정보 주체의 권익을 침해할 수 있다. 따라서 「GB/T 37025-2018 정보보안기술 - 사물인터넷 데이터 전송 보안 기술 요구 사항」 제5조에 따라 기업이 사물인터넷 관련 사업을 영위하는 경우 다음의 요구 사항을 충족시킬 것을 권장한다.

i) 데이터 전송 보안 기술 요구 사항. 「GB／T 37025-2018 정보보안기술 - 사물인터넷 데이터 전송 보안 기술 요구 사항」 제5.1조에 따라 사물인터넷의 개인정보 전송은 「GB／T 37044-2018 정보보안기술 - 사물인터넷 보안 참조 모델 및 일반 요구 사항」을 준수해야 한다. 따라서 기업은 사물인터넷을 활용하는 경우 위의 두 가지 기술 표준에 따라 상응하는 기술 요구 사항을 적용해야 한다.

ii) 개인정보 보안 단계 분류 원칙에 관한 요구 사항. 「GB／T 37025-2018 정보보안기술 - 사물인터넷 데이터 전송 보안 기술 요구 사항」 제5.3조에 따라 사물인터넷의 데이터 전송 보안 기술은 기본 단계와 고급 단계로 분류해야 하며, 자세한 내용은 아래 표와 같다.

단계	처리 내용	해당하는 개인정보
기본 단계	일반 데이터	일반 개인정보
고급 단계	중요한 데이터, 민감한 데이터, 주요 보안 문제와 관련되는 데이터	민감 개인정보

따라서 기업은 사물인터넷 시나리오에서 개인정보의 처리 범위에 따라 개인정보 보안에 대한 단계 분류가 필요한지 여부를 정하고 상응하는 보안기술 요구 사항을 적용해야 한다.

iii) 개인정보 전송 시 프라이버시 보호. 「GB/T 37025-2018 정보보안기술 - 사물인터넷 데이터 전송 보안 기술 요구 사항」 제6.3조에 따라 기업이 이용자 비밀번호, 생체 특징 정보 등의 개인정보를 처리할 때 민감 개인정보를 포함하는 경우, 이를 나타내어 표시하거나 저장하지 말아야 한다. 따라서, 사물인터넷 시나리오에서 기업은 해당 표준을 준수하는 기술적 조치를 통해 민감 개인정보를 저장해야 한다.

③ 응용계층 위험

사물인터넷 시나리오에서의 개인정보 위험은 주로 개인정보의 이용, 제공 및 삭제 위험 등을 포함하여 응용계층에 집중돼 있다. 「사물인터넷 기본 보안 표준 시스템 구축 가이드라인(2021년판)」에 따라 기업은 개인정보 처리 주요 단계의 보안에 대한 기본적인 관리와 기술적 보장을 포함하여 사물인터넷의 모든 측면에서 개인정보에 대한 안전한 통제와 사용을 보장해야 한다.

또한, 「GB/T 37044-2018 정보보안기술 - 사물인터넷 보안 참조 모델 및 일반 요구 사항」 제5.2조에 따라 기업이 사물인터넷을 운영하는 경우 애플리케이션 보안 영역을 설정하여 이용자의 신원인증, 접근권한 제어, 유지보수 등의 보안 요구 사항을 준수할 수 있다. 아울러, 애플리케이션 보안 영역은 개인정보보호를 위해 특정 네트워크 공격을 차단할 수 있는 기능을 갖추어야 한다.

다. 사물인터넷 시나리오에서 개인정보의 파기

「GB/T 37044-2018 정보보안기술 - 사물인터넷 보안 참조 모델 및 일반 요구 사항」 제5.3조에 따라 기업의 사물인터넷 응용 시스템이 만기가 되어 폐기할 때, 처리하던 개인정보에 대해 다음의 조치를 취할 수 있다.

① 기존 사물인터넷에서 수집한 개인정보, 접속로그 등의 정보를 제때에 백업하거나 파기할 수 있다.

② 사물인터넷 장치를 재사용해야 하는 경우, 사전에 해당 장치를 초기화 설정하고 캐시된 개인정보를 파기하여 기존 사물인터넷 시스템의 개인정보가 유출되는 것을 방지해야 한다.

유의 사항
사물인터넷은 비교적 넓은 개념이므로 「개인정보 보호법」과 기업이 속한 산업의 특별 규정에 따라 사용 중인 사물인터넷 시스템을 점검하여 법령이나 요구 사항에 적합하지 않는 부분을 시정 또는 갱신해야 한다.

법률 안내
사물인터넷 시나리오에서 「개인정보 보호법」 규정을 준수하는 것 외에 다음의 법규와 표준을 함께 참조할 것을 권장한다. - 「사물인터넷 기본 보안표준 시스템 구축 가이드라인(2021년판)」 - 「GB/T 37044-2018 정보보안기술 - 사물인터넷 보안 참조 모델 및 일반 요구 사항」 - 「GB/T 37025-2018 정보보안기술 - 사물인터넷 데이터 전송 보안 기술 요구 사항」 - 「GB/T 37024-2018 정보보안기술 - 사물인터넷 감지계층 게이트웨이 보안기술 요구 사항」 - 「사물인터넷 감지계층 통신망 연결 보안 요구 사항 GB/T 37093-20」

제 4절 차량인터넷 운영 시나리오

차량인터넷은 차내망, 차량 간 네트워크 및 차량 내 인터넷을 기반으로 차량과 X(X: 차량, 도로, 보행자 및 인터넷 등) 간에 당사자가 합의한 통신 프로토콜, 데이터 및 개인정보의 상호작용 표준에 따라 무선통신 및 정보교환을 진행하는 시스템 네트워크를 의미한다. 다시 말해, 차량인터넷은 교통 시스템 분야에서 사물인터넷 기술의 전형적인 적용이다.

차량인터넷과 관련되는 개인정보 및 데이터는 주로 다음과 같은 두 가지 유형으로 나눈다.

유형	내용
이용자 관련 정보 및 데이터	· 신원정보(예: 성명, 증빙서류 종류 및 번호, 나이, 성별, 직업, 직장, 주소, 국적, 전화번호 등) · 차량 이용 시 생성되는 이용자 행위 데이터(예: 운전 및 주행 안전 서비스 정보, 생활 서비스 정보, 연락처 정보, 조작일지 등) · 지문, 음성, 얼굴 영상 등 기타 개인정보
차량 관련 데이터	· 차량 기본 자료(예: 차종, 브랜드, 모델, 섀시모델, 엔진번호, 연료종류, 차량번호, 차량식별코드 등) · 차량 보조 또는 자율주행 소프트웨어 및 하드웨어 데이터

	· 차량 외부 데이터 · 차량 내비게이션 데이터 · 자율주행을 위한 고정밀 지도 위치측정 데이터

차량인터넷 적용 시나리오에서 기업은 많은 양의 개인정보를 수집하게 될 것이며, 그 중에는 민감 개인정보와 국가에서 엄격하게 통제하는 중요한 데이터도 포함될 수 있다. 따라서 차량인터넷 시나리오에서 개인정보를 처리하는 기업은 다음과 같은 준법 사항에 유의할 것을 권장한다.

가. 개인정보의 범주 및 등급 분류

① 차량인터넷 개인정보 범주 및 등급 분류에 대한 특별 요구 사항

i) 「산업데이터 범주 및 등급 분류 가이드라인(시범시행)」에서 규정하는 분류 : 「산업데이터 범주 및 등급 분류 가이드라인(시범시행)」에 따라 자동차 산업에 속한 기업은 관련 데이터에 대해 범주 및 등급을 분류해야 할 필요가 있다. 위의 지침은 산업데이터를 변조, 파괴, 유출 또는 불법으로 사용하여 산업생산 및 경제적 이익 등에 미칠 수 있는 잠재적 영향을 기준으로 산업데이터를 3단계로 분류하고 있으며, 그 중에서 개인정보에 대한 구분 기준은 다음과 같다.

단계	기준
3단계	국민경제, 산업발전, 공공이익, 사회질서 내지는 국가안보에 중대한 영향을 미치는 경우
2 단계	유발하는 캐스케이드 효과(파급효과)가 분명하고, 영향이 미치는 범위가 다양한 산업, 지역 또는 해당 산업 내의 다수 기업과 관련되거나, 또는 영향이 장기간 지속되거나, 또는 다수의 공급업체 및 고객 자원이 불법으로 취득되거나 대량의 개인정보가 유출되는 경우
1 단계	영향을 받는 이용자와 기업의 수가 적고, 생산 및 생활 영역이 제한적이며, 지속 시간이 짧은 경우

따라서 기업은 차량인터넷 적용 시나리오에서 이 지침에 따라 개인정보의 단계를 구분하고, 각 단계별 요구 사항에 맞는 보호조치를 취할 수 있다.

ii) 「차량 데이터 보안에 관한 약간의 규정(시범시행)」에 따른 분류 요구 사항 : 「차량 데이터 보안에 관한 약간의 규정(시범시행)」 제3조 제6항에 따라 중요 데이터란 일단 변조, 파괴, 유출 또는 불법 취득, 이용 시 국가안보, 공공의 이익 또는 개인, 조직의 적법한 권익을 침해하는 데이터를 말한다.

따라서, 차량 데이터 처리자는 본 조에 따라 기업의 중요 데이터의 범위를 정해야 한다. 「개인정보 보호법」, 「차량 데이터 보안에 관한 약간의 규정(시범시행)」, 「차량인터넷 정보 서비스 - 데이터 보안 기술 요구 사항」 및 「차량인터넷 정보 서비스 - 이용자 개인정보보호 요구 사항」을 종합 분석하여 전반적으로 차량 데이터를 다음 두 가지 범주로 구분할 수 있다.

차량 관련 데이터		개인정보	
일반 데이터	차량번호, 차량모델, 차량 평균 주행속도, 노면상태, 도로혼잡 상황 등	일반 개인정보	전화번호, 이메일 주소, 충돌방지 경고 서비스 중의 개인정보 등
중요 데이터	- 중요하고 민감한 지역의 지리, 인파 및 차량흐름 데이터 - 경제운용 상황을 반영한 데이터 - 차량 충전망 운영 데이터 - 얼굴, 번호판 등을 포함한 차량 외부 동영상 및 이미지 데이터 - 100,000명 이상의 개인정보 주체에 관한 개인정보 - 기타	민감 개인정보	- 개인 생체인식 정보: 지문, 손금, 얼굴, 성문(聲紋), 얼굴윤곽 등 - 개인 신원 정보: 신분증, 사회보장카드, 운전면허증 - 차량 위치 및 궤적 - 운전자 또는 승객의 음성 및 동영상 - 차량인터넷 거래: 거래 계정 및 비밀번호, 거래 기록

따라서 기업은 관련 법률, 규정, 표준 및 자체 상황에 비추어 수집하는 데이터 가운데 어떤 데이터가 중요 데이터에 해당하는지를 판단하고, 중요 데이터 보호에 필요한 조치를 취해야 한다.

나. 개인정보 처리에 대한 특별 요구 사항

① 개인정보 처리에 대한 특별 원칙을 명확히 해야 한다.

「차량 데이터 보안에 관한 약간의 규정(시범시행)」 제6조에서는 차량 데이터 처리자가 차량 데이터 처리활동을 수행할 때 참조할 수 있는 원칙을 제시하였다.

i) 차량 내부 처리 원칙. 꼭 필요한 경우를 제외하고 관련 개인정보를 차량 외부로 제공하지 말아야 한다. 「차량 데이터 보안에 관한 약간의 규정(시범시행)」에서는 “차량 내부” 및 “차량 외부”라는 영역 개념을 추가하였다. 해당 규정 제6조 및 제8조에 따라 차량 데이터 처리자가 개인정보

및 중요 데이터를 처리하는 경우, 차량 내부에서 처리하는 원칙을 준수해야 하며, 꼭 차량 외부로 제공해야 하는 경우에는 가능한 익명화 처리해야 한다.

ii) 묵시적 불수집 원칙. 운전자가 자발적으로 수집 상태로 설정하지 않는 한 운전자가 매번 운전을 시작할 때마다 시스템은 기본적으로 불수집 상태로 설정되어야 한다.

iii) 정확도 적용 범위 원칙. 기업에서 제공하는 기능성 서비스의 데이터 정확도 요구에 따라 관련 장치(예: 카메라, 레이더) 등의 적용 범위와 해상도를 정해야 한다.

iv) 탈민감 처리 원칙. 기업은 가능한 한 관련 개인정보를 익명화 처리하거나 비식별화 처리해야 한다.

② 개인정보 처리를 진일보 제한하는 규칙 : 기업이 차량인터넷 사업을 영위하는 경우, 「개인정보 보호법」에 규정된 개인정보 처리 규칙을 준수하는 것 외에도 「차량 데이터 보안에 관한 약간의 규정(시범시행)」 제7조에 따라 개인정보를 처리할 때 이용자 가이드북, 차량용 디스플레이 패널, 음성 및 기타 차량 응용프로그램 등을 이용한 분명한 방식으로 다음 사항을 개인정보 주체에게 알려야 한다.

i) 차량 궤적, 운전습관, 음성, 동영상, 이미지 및 생체인식 특징 정보 등을 포함한 개인정보의 처리 종류

ii) 개인정보를 수집하는 구체적인 시나리오와 수집을 중단하는 방법 및 수단

iii) 개인정보 처리 목적, 용도 및 방법

iv) 개인정보의 보관장소, 보관기간 또는 그런 보관장소, 보관기간을 정하는 규칙

v) 개인정보 조회 및 복사, 차량 내부 관련 개인정보 삭제, 이미 차량 외부로 제공된 개인정보에 대한 삭제 요청 방법 및 수단

vi) 개인정보 주체가 권리행사 시 연락할 수 있는 담당자의 성명 및 연락처

vii) 그 밖에 법률 및 행정법규에서 정하는 바에 따라 고지해야 하는 사항

아울러, 「차량 데이터 보안에 관한 약간의 규정(시범시행)」 제8조에 따라 차량 데이터 처리에 대한 동의는 「개인정보 보호법」 및 관련 법령을 준수해야 한다. 기업이 주행안전을 확보하기 위한 필요한 경우로서 개인정보 주체로부터 동의를 얻을 수 없는 상황에서 차량 외부의 개인정보를 수집하고 차량 외부로 제공하는

경우, 자연인을 식별할 수 있는 화면을 삭제하거나 화면 내의 얼굴 정보 등에 대한 국부적인 윤곽화 처리를 포함하여 관련 개인정보를 익명화 처리해야 한다.

③ 민감 개인정보 처리 요구 사항 구체화 : 차량인터넷 시나리오에서 차량 궤적, 음성, 동영상, 이미지 및 생체인식 특징 정보 등은 민감 개인정보의 범위에 포함될 수 있다. 「차량 데이터 보안에 관한 약간의 규정(시범시행)」 제9조에 따라 차량인터넷을 활용하여 민감 개인정보를 처리하는 경우, 법령이나 국가의 강제성 기준에서 달리 규정하지 않는 한 다음의 요구 사항을 충족해야 한다.

i) 민감 개인정보 처리는 주행안전 강화, 운전보조, 내비게이션 등을 포함하여 개인에게 직접 서비스를 제공하기 위한 목적이어야 한다.

ii) 기업은 이용자 가이드북, 차량용 디스플레이 패널, 음성 및 차량용 응용프로그램 등을 통해 민감 개인정보 처리의 필요성 및 개인정보 주체에 대한 영향을 분명한 방식으로 명확하게 알려야 한다.

iii) 민감 개인정보를 처리하는 경우, 개인으로부터 별도의 동의를 얻어야 하는 동시에 개인정보 주체가 자율적으로 동의기한을 설정할 수 있어야 한다.

iv) 주행안전을 보장하는 전제 하에 적절한 방식으로 수집 상황을 개인정보 주체에게 안내하여 수집을 해지할 수 있도록 편의를 제공해야 한다.

v) 개인정보 주체가 민감 개인정보에 대해 삭제를 요청하는 경우, 차량 데이터 처리자는 근무일 기준 10일 이내에 해당 개인정보를 삭제해야 한다.

유의 사항
「개인정보 보호법」에서 민감 개인정보의 삭제기한에 대해 규정하지 않고 있기 때문에, 차량인터넷 시나리오에서 기업은 각종 법률, 규정 및 기준을 참조하여 다음과 같이 개인정보 삭제기한을 확인해야 한다. - 「정보보안기술 - 커넥티드 차량 데이터 수집 보안 요구 사항(초안)」 제6조에 따라 커넥티드 차량 시나리오에서 커넥티드 차량이 수집한 차량 위치 및 궤적 관련 데이터는 차내 저장장치, 원격 정보 서비스 플랫폼(TSP)에서 7일 이상 보관할 수 없다. - 「차량 수집 데이터 처리 보안 가이드라인」 제6.1조 및 제6.2조에 따라 차량 데이터 수집 시나리오에서 특정 조건을 충족하지 않는 한 차량 외부 데이터, 위치 및 궤적 데이터를 원격 정보 서비스 플랫폼 등 차량 외부에서 14일 이상 보관할 수 없다.

④ 중요 데이터 처리에 관한 특별 의무 제시 : 기업이 차량인터넷 시나리오에서 처리하는 개인정보가 중요 데이터에 해당하는 경우, 다음 요구 사항을 준수해야 한다.

i) 유관 부서에 위해성 평가 보고서 제출 의무 : 「차량 데이터 보안에 관한 약간의 규정(시범시행)」 제10조에 따라 기업의 데이터 처리활동에 중요 데이터가 포함되는 경우, 규정에 따라 위해성을 평가하고 성•자치구•직할시의 네트워크정보 당국과 유관 부서에 위해성 평가 보고서를 제출해야 한다. 이에 관한 자세한 내용은 다음과 같다.

- 중요 데이터의 종류, 수량, 범위, 보관 장소 및 기한, 이용방법
- 기업의 데이터 처리활동 수행 상황 및 제3자 제공 여부
- 기업이 당면한 데이터 보안 위험 및 대응책 등

ii) 정기적으로 유관 부서에 연간 차량보안관리 상황 보고 의무 : 「차량 데이터 보안에 관한 약간의 규정(시범시행)」 제13조에 따라 기업이 중요 데이터 처리활동을 수행하는 경우, 매년 12월 15일 이전에 성•자치구•직할시 네트워크정보 당국 및 유관 부서에 연간 차량 데이터 보안관리 상황을 보고해야 한다. 구체적인 제출 내용은 다음과 같다.

- 차량 데이터 보안관리 책임자 및 이용자 권익 담당자의 성명 및 연락처
- 처리하는 차량 데이터의 종류, 규모, 목적 및 필요성
- 보관 장소 및 기한 등을 포함한 차량 데이터의 안전보호 및 관리조치
- 국내 제3자에게 차량 데이터 제공 상황
- 차량 데이터 보안사고 및 조치 상황
- 차량 데이터 관련 이용자 불만사항 및 처리 상황
- 국가네트워크정보 당국이 국무원 산하 공업정보화, 공안, 교통운수 및 기타 유관 부서와 공동으로 정한 기타 차량 데이터 보안관리 상황

따라서, 차량인터넷 관련 기업은 본 조의 규정에 따라 제때에 유관 부서에 위의 내용이 포함된 차량보안관리 연간 보고서를 제출해야 한다.

iii) 중요 데이터의 국내 보관 및 국외 이전에 관한 의무 : 「차량 데이터 보안에 관한 약간의 규정(시범시행)」에 따라 기업이 중요 데이터를 국외로 이전하는 경우, 다음의 요구 사항을 충족해야 한다.

- 중요 데이터의 국내 보관 및 국외 이전에 대한 안전성 평가 의무를 책임져야 한다. 「차량 데이터 보안에 관한 약간의 규정(시범시행)」 제11조에 따라 중요

데이터는 국내에 보관해야 하며, 만약 국외로 이전해야 하는 경우에는 네트워크정보 당국이 주관하는 데이터의 국외 이전에 대한 안전성 평가를 통과해야 한다.

- 중요 데이터의 국외 이전 후의 처리 범위에 대한 엄격한 제한. 「차량 데이터 보안에 관한 약간의 규정(시범시행)」 제12조에 따라 기업이 중요 데이터를 국외로 이전하는 경우, 위에서 언급한 안전성 평가에 명시된 목적, 범위, 방법 및 데이터의 종류, 규모를 초과하지 않아야 한다.
- 중요 데이터의 국외 이전에 대한 규제 당국의 정기적인 불시검사. 「차량 데이터 보안에 관한 약간의 규정(시범시행)」 제12조에 따라 국가네트워크정보 당국은 국무원 유관 부서와 공동으로 위에서 언급한 중요 데이터의 국외 이전 후의 처리 행위에 대해 불시검사를 진행할 수 있다. 이때, 기업은 협력하는 동시에 관련 자료를 제출해야 한다.

유의 사항
기업이 중요 데이터의 국외 이전과 관련되는 경우, 매년 연간 차량 데이터 보안관리 상황을 성•자치구•직할시의 네트워크정보 당국과 유관 부서에 보고할 때 다음의 내용도 함께 보고해야 한다. ✓ 국외에서 중요 데이터를 이전 받는 자의 기본적인 상황 ✓ 국외로 이전하는 차량 데이터의 종류, 규모, 목적 및 필요성 ✓ 차량 데이터의 국외 보관 장소, 기한, 범위 및 방법 ✓ 국외로 이전하는 차량 데이터에 대한 이용자 불만사항 및 처리 상황 등

다. 개인정보의 국외 이전

차량인터넷 시나리오에서 개인정보가 관련되는 경우, 기업은 「개인정보 보호법」 제38조 ~ 제40조 개인정보의 국외 이전에 관한 규정[26] 및 기타 법령에 따라 준법의무를 이행해야 하며, 그 의무는 다음 사항을 포함하되 이에 국한되지 아니한다.

① 국외로 이전하는 개인정보는 개인정보 주체로부터 별도의 동의를 얻어야 한다.

② 로컬 보관 의무 이행 및 네트워크정보 당국에서 주관하는 국외 이전 전 안전성 평가를 통과해야 한다.

③ 국외의 이전 받는 자가 「개인정보 보호법」에 따른 동일한 보호 수준을 준수할 수 있도록 국외 이전 표준계약을 체결하거나 인증을 취득해야 한다.

법률 안내

26) 국외 이전 관련 내용은 본 가이드북 제3장 개인정보 준법 구조 제3.6절 개인정보의 국외 이전 중 제1항 개인정보 국외 이전 시나리오 및 제2항 개인정보 국외 이전에 관한 기본 규칙을 참조.

「개인정보 보호법」의 관련 규정을 준수하는 것 외에 다음과 같은 법률, 규정 및 기준을 참고할 것을 권장한다.
- 「도로교통안전법」
- 「차량 데이터 보안에 관한 약간의 규정(시범시행)」
- 「차량인터넷 정보 서비스 - 데이터 보안 기술 요구 사항」
- 「차량인터넷 정보 서비스 - 이용자 개인정보보호 요구 사항」
- 「지능형 커넥티드 차량 일반도로 시범운행 및 시범응용 관리 규범(시범시행)」
- 「지능형 커넥티드 차량 제조사 및 제품 진입 관리 강화에 관한 의견」
- 「정보보안기술 - 커넥티드 차량 데이터 수집 보안 요구 사항(초안)」
- 「차량인터넷(지능형 커넥티드 차량) 네트워크안전 표준 시스템 구축 가이드라인(의견수렴안)」
- 「차량인터넷(지능형 커넥티드 차량) 네트워크안전 업무 강화에 관한 통지(의견수렴안)」

제 5절 금융서비스 제공 시나리오

기업이 금융서비스업을 영위하는 경우에도 금융서비스의 특수성으로 인해 개인의 재산에 직접적인 영향을 미치는 개인금융정보를 수집해야 경우가 많기 때문에 개인정보보호 및 처리에 특히 주의를 기울여야 한다.

가. 개인금융정보 범주 및 등급 분류

기업은 개인정보가 유출되거나 변조될 시 개인정보 주체에게 미치는 위해성 수준에 따라 범주 및 등급을 분류해야 한다. 아울러, 다양한 표준 및 규정에 따라 개인금융정보에 대한 범주 및 등급 분류 기준이 다르며, 자세한 내용은 다음과 같다.

① 「JR/T 0171-2020 개인금융정보 보호기술 규범」에서 규정하는 범주 및 등급 분류

「JR/T 0171-2020 개인금융정보 보호기술 규범」은 개인금융정보의 민감도를 높은 수준에서 낮은 수준으로 C3, C2, C1 세 가지 종류로 구분한다. 금융업에 종사하는 기업은 위 기술규범의 요구 사항에 따라 개인금융정보에 대해 범주 및 등급을 분류할 수 있다.

유의 사항

- 「JR/T 0171-2020 개인금융정보 보호기술 규범」에서 규정하는 개인금융정보의 분류
  - (ㄱ) C3: 개인정보 주체의 식별정보를 말하며 정보 유출 시 직접적인 재산 피해를 초래할 수 있다.
  - (ㄴ) C2: 특정 개인금융정보 주체의 신원 및 금융상태를 식별할 수 있는 개인금융정보와 금융 상품 및 서비스에 사용되는 핵심정보를 말하며, 유출 시

간접적인 재산피해, 차별적 대우 또는 정보보안에 위협이 될 수 있다.

(ㄷ) C1: 금융기관에서 내부적으로 사용하는 개인금융정보를 말한다.

- 개인금융정보의 조합

개인금융정보 주체가 제공하는 가족 구성원 정보는 앞서 언급한 민감도에 따라 분류해야 한다. 다양한 낮은 수준의 정보일지라도 조합, 연계 또는 분석을 통해 높은 민감도의 정보를 구성할 수 있다. 구체적인 서비스 시나리오 및 시나리오에서 관련 정보의 역할을 기반으로 정보를 식별하고 분류하여 맞춤형 보호조치를 취할 수 있다.

② 「JR/T 0197-2020 금융데이터 보안등급 분류 가이드라인」에서 규정하는 범주 및 등급 분류

「금융데이터 보안등급 분류 가이드라인」은 보다 넓은 의미에서 금융데이터를 분류하고 보호할 것을 규정하였다. 상기 지침에 따라 금융데이터를 5개 단계로 분류하고, 그 중에서 단계 5는 최고 수준, 단계 1은 최저 수준 금융데이터를 의미한다. 기업은 단계별 금융데이터에 대한 요구 사항에 따라 해당하는 보호조치를 취할 수 있다.

유의 사항
「JR/T 0197-2020 금융데이터 보안등급 분류 가이드라인」의 분류 규정에 따라 단계별 개인정보의 범주 및 등급 분류 기준은 다음과 같다. - 단계 5: 국가안보에 영향을 미치거나 공공의 이익에 중대한 영향을 미치는 정보 - 단계 4: 개인정보 주체의 권익에 중대한 영향을 미치는 정보 - 단계 3: 개인정보 주체의 권익에 일반 수준의 영향을 미치는 정보 - 단계 2: 개인정보 주체의 권익에 경미한 수준의 영향을 미치는 정보 - 단계 1: 개인정보 주체의 권익에 영향을 미치지 않는 정보 관련 예시는 본 절의 “(3) 표준별 개인금융정보 분류” 표를 참조한다.

③ 표준별 개인금융정보 분류

다양한 기술 표준과 요구 사항에 따라 개인금융정보가 속하는 범주와 단계를 다음과 같이 요약하고 정리하였다.

분류	JR/T 0197	JR/T 0171	GB/T 35273
• **기존의 식별정보**(은행카드 마그네틱 데이터(또는 칩 등 유사 정보), 카드 인증코드(CVN 및 CVN2), 카드 유효기간, 은행카드 비밀번호, 인터넷 결제 비밀번호, 계정 로그인 비밀번호, 거래 비밀번호, 조회 비밀번호 등) • **일반 프라이버시 생체특징 정보**(얼굴, 성문, 걸음걸이(步態), 귀모양, 눈주름, 필적 등) • **중요 프라이버시 생체특징 정보**(지문, 홍채 등)	**단계 4**	C3	**민감 개인정보**

• **개인 기본 정보**(성명, 성별, 국적, 민족, 혼인, 증빙서류, 주소 등) • **개인 재산 정보**(소득, 부동산, 차량, 납세액, 공공적립금, 사회보험, 의료보험 등) • **개인 연락 정보**(전화번호, 이메일 주소, 위챗 계정 등) • **개인 건강 및 생리 정보**(병증, 입원일지, 진료지시서, 검사보고서, 수술 및 마취 기록, 간호기록, 투약기록, 알레르기 정보, 출산정보, 병력, 진찰 및 치료 상황, 가족병력, 전염병 병력 등) • **개인의 지리적 위치정보**(국가, 도시, 지역, 도로, 경위도 등) • **개인 식별 보조정보**(동적 비밀번호, SMS 인증번호, 비밀번호 찾기 문제 답안, 동적 성문 비밀번호 등) • **개인 신용 정보**(대출정보, 상환정보, 부채정보) • **개인 간 관계 정보**(부모, 자녀, 형제자매, 배우자, 사회적 관계) • **기본적인 태그 정보**(교육, 직업 등 기본 속성을 기반으로 구축한 개인태그) • **관계 태그 정보**(가족 관계, 직업 관계, 비즈니스 관계 등 연관 속성을 기반으로 구축한 개인태그)	**단계 3**	C2	**민감 개인정보/개인정보**
• **개인 교육 정보**(학교, 대학/학부, 학력, 학위, 학과, 입학날짜, 졸업날짜 등) • **개인 직업 정보**(직장, 직위, 근무장소, 소득, 시작시간, 종료시간 등) • **개인 자격증 정보**(증서번호, 발급기관, 발효일, 마감일 등) • **개인 정당 정보**(당파, 가입시간) • **공사(公私) 간 관계 정보**(직무정보) • **개인 행위 정보**(온•오프라인 상담, 구매, 사용 기록; 열람기록, 운전습관 등) • **기타 태그**(서명태그, 거래태그, 행위태그, 마케팅 서비스 태그, 위험태그, 가치태그)	**단계 2**	C1	**개인정보**

나. 개인금융정보 보호 조직기구 설립

① 개인금융정보 보호 조직기구 및 직무 설정

기업이 금융서비스업을 영위하는 경우, 「개인정보 보호법」 제52조에 따라 개인정보보호책임자를 선임할 필요가 있는지 확인하는 동시에, 「JR/T 0171-2020 개인금융정보 보호기술 규범」 제7조에 따라 개인금융정보 보호 조직기구를 설립해야 한다.

유의 사항

「JR/T 0171-2020 개인금융정보 보호기술 규범」 제7조에 따라 기업이 선임하고 설립한 개인금융정보 보호 책임자와 개인금융정보 보호 책임기구는 일반적으로 다음과 같은 직책을 갖는다.

- 기업의 개인금융정보 보안관리 제도 제정 및 관리를 책임진다.
- 이와 함께, 「개인정보보호정책」 및 관련 규정을 제정, 시행 및 정기적으로 업데이트한다.
- 기업 내부 및 외부 협력사의 개인금융정보 보안관리를 감독한다.
- 개인금융정보 보안관리에 대한 내부감사 수행 및 개인금융정보 보안사건을 분석하고 처리한다.
- 개인금융정보 보안 영향평가를 실시하고 개인금융정보 보호대책을 건의한다.
- 알 수 없는(금융상품, 서비스 기능 및 개인정보처리방침에 위배) 개인금융정보가 처리되는 것을 방지하기 위해 금융 상품 또는 서비스를 출시하기 전에 기술적 테스트를 실시한다.
- 개인금융정보 주체가 불만사항 제기 및 이의 신청할 수 있는 방법 등을 공개하고 개인금융정보 관련 불만사항 및 이의 신청을 신속하게 수리한다.

② 「JR/T0223-2021 금융데이터보안 - 데이터 수명주기 보안 규범」에서 규정하는 조직기구 관련 요구 사항

금융회사는 「JR/T0223-2021 금융데이터보안 - 데이터 수명주기 보안 규범」 제8조의 “데이터 보안 조직기구 보장”에 관한 규정에 따라 데이터보안 관리위원회를 구성하고 의사결정, 관리, 실행 및 감독을 포함하는 하향식 데이터 보안 관리 시스템을 구축함으로써, 조직기구와 직무 설정을 명확히 하고 데이터 수명주기 보안 요구 사항을 효과적으로 이행해야 한다.

시스템	조직계층	구성
금융정보 보안 관리 시스템	의사결정층	• 데이터보안관리위원회 임원진 또는 관리그룹(있을 시) • 기구 내 고위 관리층
	관리층	• 데이터보안관리위원회 구성원 • 기술, 업무, 법무, 위험 관리 등 주요 책임자
	실행층	• 기술, 업무, 법무, 위험 관리 등 직무 담당자
	감독층	• 감사, 검사 등 유관 부서 담당자

따라서 기업은 법률, 규정, 표준 및 실무 수요에 따라 개인금융정보 보호 관련 부서 및 조직을 구성하여 기업에서 처리하는 개인금융정보를 보호해야 한다.

다. 개인금융정보 전 수명주기 관리 시스템 구축

「개인정보 보호법」 제4조에서 개인정보 처리가 개인정보의 수집•보관•이용•가공•전송•제공•공개•삭제 등의 활동을 포함함을 명시함으로써 개인정보의 전 수명주기를 아우른다. 따라서, 금융회사는 개인금융정보의 전 수명주기를 포함하는 관리 시스템을 구축해야 개인금융정보 처리의 모든 측면에서 「개인정보 보호법」의 기준을 충족시킬 수 있다. 「개인정보 보호법」의 기본 규정 외에도 개인금융정보에 대한 전 수명주기 관리 시스템을 보다 철저하게 구축하기 위해 다음의 표준, 지침 또는 규범을 참고할 수 있다.

① 「JR/T 0171-2020 개인금융정보 보호기술 규범」 제6조, 제7조는 개인금융정보의 수명주기에 대해 기술적 및 관리적 요구 사항을 제시하였다.

② 「JR/T0223-2021 금융데이터보안 - 데이터 수명주기 보안 규범」은 수명주기 관점에서 개인금융정보에 대한 보다 완전하고 체계적인 보안 요구 사항을 제시하였다.

유의 사항
「개인정보 보호법」과 앞서 언급한 표준 및 규범에 따라 개인금융정보의 전 수명주기 관리에서 다음의 사항에 유의해야 한다. - **정보수집:** 개인정보처리방침의 대상이 되는 개인금융정보 주체의 명시적인 동의 및 정보 출처의 추적성을 확보할 것을 요구함과 더불어, 처리단말, 클라이언트 애플리케이션 및 브라우저 등의 방식을 통해 이용자에게 은행카드 비밀번호, 인터넷 결제 비밀번호 입력(또는 설정)을 유도하는 경우, 비밀번호가 일반 텍스트로 표시되지 않도록 노출을 제한하는 조치를 취해야 하며, 기타 비밀번호에 해당하는 정보도 마찬가지로 노출을 제한하는 조치를 취해야 한다. - **정보전송:** 개인금융정보 전송 참여자(데이터 수신자 포함)는 정보의 기밀성, 무결성 및 가용성을 보장해야 한다. 예를 들어, 개인금융정보를 전송하기 전에 양 통신 당사자는 효과적인 기술적 수단을 통해 신원 식별 및 인증을 수행해야 하고, 개인금융정보 수신자는 수신한 정보에 대해 무결성 점검을 수행해야 한다. - **정보보관:** 기업이 관련 금융서비스를 중단하는 경우, 보관하고 있던 개인금융정보를 국가의 법령 및 업계 주관부서의 관련 규정에 따라 적절하게 처리하는 외에, 국가 또는 업계 주관부서에서 지정한 기관으로 이전하여 계속 보관할 수 있다. - **정보이용(또는 표시):** 앞서 언급한 표준 기술규범은 업무 처리 및 조회 기능을 제공하는 애플리케이션, 애플리케이션 백엔드 관리 및 업무 지원 시스템의 표시에 대한 기술적 요구 사항을 제시하였다. 특히, 기타 개인금융정보 주

체와 관련된 정보일지라도 특별한 경우를 제외하고는 노출을 제한하여 표시하는 것이 좋다.

- **정보 공유 및 이전:** 법령에 따른 보안 영향평가, 데이터보호책임계약 체결, 접근제어, 감사 등을 제외하고, 기업의 정보를 공유 및 이전할 때 결제 토큰 기술 등 탈민감화 기술로 개인금융정보를 처리해야 한다.
- **정보의 위탁처리:** 위탁처리하는 개인금융정보는 비식별화(암호화 기술만 적용하지 말 것) 등의 방식으로 탈민감 처리해야 한다.
- **정보파기:** 개인정보 파기에 대한 파기관리 시스템 구축, 관련 기록 보관 등 통상적인 처리 요구 외에 개인금융정보를 저장하고 있는 매체를 더 이상 사용하지 않을 경우, 비가역적인 방식(예: 자장 제거, 소각, 분쇄 등)으로 해당 매체를 파기 처리해야 한다. 개인금융정보가 저장되어 있는 매체를 계속해서 사용해야 하는 경우에는 인덱스 삭제나 파일 시스템 삭제만으로 정보를 파기해서는 안 되며, 반복적 덮어쓰기 등의 방식으로 안전하게 삭제하여 매체 내의 개인금융정보가 복구 불능하거나 기타 방식으로 더 이상 이용할 수 없도록 해야 한다.

라. 개인금융정보 영향평가 시스템 개선

「개인정보 보호법」 제55조에 따르면, 기업은 자체 실정에 따른 개인정보 영향평가 시스템을[27] 구축해야 한다. 「GB/T 39335-2020 개인정보 보안 영향평가 지침」 부록 B에 개인정보 처리활동의 고위험 시나리오들을 열거하였다. 따라서 다음과 같은 고위험 개인금융정보 처리 시나리오에 유의할 것을 권장한다.

① 데이터 처리가 개인정보 주체에 대한 평가 또는 평점, 특히 개인정보 주체의 업무태도, 경제상황, 건강상태, 취향 및 취미에 대한 평가 또는 예측(예: 금융회사의 대출 전 고객신용 분석, 보험회사의 고객 생활방식 및 건강상태를 고려한 보험료 설정 등)

② 개인정보를 이용한 자동분석을 통해 사법 판결을 내리거나 기타 개인에 중대한 영향을 미치는 결정(예: 금융회사가 이용자 프로파일을 통해 이용자의 특정 취향을 대상으로 한 자산관리 계획을 설정하고 이용자에게 추천하는 경우)

③ 민감함 개인정보의 수집량이 많고, 수집 빈도가 높으며, 이용자의 재무상태 등과 밀접하게 연관되는 경우

④ 다양한 처리활동에 따른 데이터 세트를 매칭 및 병합하여 경영에 이용하는 경우(예: 금융회사가 사기방지, 위험통제 등을 위해 이용자의 최근 5년 동안의 개인정보를 병합하는 경우)

27) 개인정보보호 영향평가 관련 내용은 본 가이드북 제3장 개인정보 준법 구조의 제3.5절 기업의 의무 중 제4항 개인정보보호 영향평가 의무를 참조.

⑤ 금융데이터 처리가 미성년자, 환자, 노인, 저소득층 등 취약계층과 연관되는 경우
⑥ 생체인식, 인공지능 등을 포함하되 이에 국한되지 않는 혁신적인 기술 적용 (예: 금융업계의 인공지능 기반 고객 서비스 기능 및 지문인식 기능)

따라서 기업은 앞서 언급한 고위험 시나리오에 있어 보다 엄격한 개인금융정보 보호조치를 취하여 개인금융정보 처리의 위험을 줄일 수 있다.

마. 개인금융정보 보호 준법감사제도 구체화

「개인정보 보호법」 제54조에 따르면, 개인정보처리자는 정기적으로 준법감사 의무를 이행해야 한다. 앞서 언급한 법적 요구 사항, 「JR/T0223-2021 금융데이터 보안 - 데이터 수명주기 보안 규범」 제8조 및 업계 사례에 따라 금융회사 감사 부서의 감사 업무 중 다음 사항을 포함할 것을 권장한다.

① 금융회사의 실제 업무에 따라 감사 주기, 방법, 형식 등을 포함하는 감사 정책 및 규범을 정해야 한다.
② 개인금융정보 보안에 대한 내부 감사 및 분석을 수행하고, 문제점과 위험을 신속하게 파악하고 피드백하며, 금융회사의 사후 정비업무를 감독한다.
③ 외부 제3자 감사기관의 협력이 필요한 경우, 외부감사 관련 준비 및 조율 업무에 협조해야 한다.

바. 개인금융정보 보호 교육 및 훈련 제도 시행

「개인정보 보호법」 제51조에 따르면, 기업은 개인정보보호 종사자에 대해 정기적으로 보안 교육 및 훈련을 실시해야 한다. 「JR/T0223-2021 금융데이터보안 - 데이터 수명주기 보안 규범」 제8조 규정을 중심으로, 기업이 개인정보 보안 교육 및 훈련을 실시할 때 다음 사항에 유의할 것을 권장한다.

① 교육계획에 따라 정기적으로 데이터 보안 인식 교육 및 훈련을 실시해야 한다. 교육 내용에는 국가의 관련 법령, 금융업 관련 규정, 제도, 기술표준, 업계 사례 및 개인정보 보안 관련 사내 제도 및 관리절차 등을 포함하되 이에 국한되지 아니한다. 아울러, 관련 교육 결과를 평가, 기록 및 보관해야 한다.
② 보안등급이 높은 개인금융정보에 밀접하게 접근하는 종사자에 대한 교육을 통해 개인금융정보의 주기적인 삭제 인식을 제고하고, 개인금융정보 삭제에 대한 정기적인 자체점검을 실시해야 한다.

③ 개인금융정보 보안관리 전임 및 주요 직책 담당자에 대해 매년 1회 이상 특별 교육을 실시해야 한다.

④ 금융회사는 「개인정보보호정책」에 중대한 변화가 발생했을 때, 주요 직책을 담당하는 직원에 대한 전문 교육 및 고과를 실시하여 해당 인력이 관련 내용을 숙지하도록 해야 한다.

사. 개인금융정보의 국외 이전에 관한 안전성 평가 시스템 구축

기업이 금융서비스를 제공할 때 개인정보의 국외 이전에 관한 「개인정보 보호법」 제38조 ~ 제43조의 규정을 준수하는 것 외에, 「JR/T 0171-2020 개인금융정보 보호기술 규범」 제7조의 개인금융정보 국외 이전에 관한 특별 요구 사항도 유의해야 하며 자세한 내용은 다음과 같다.

① 국내 보관 의무: 기업이 중국 국내에서 금융 상품 또는 서비스를 제공하는 과정에서 수집 및 생성한 개인금융정보는 중국 국내에서 보관, 처리 및 분석하는 것을 원칙적으로 한다. 즉, 관련 개인금융정보 처리 행위가 꼭 필요한 경우가 아니라면 개인금융정보를 국외로 이전하지 말아야 한다.

② 업무상 필요에 따른 국외 이전: 기업이 금융서비스를 제공하면서 꼭 개인금융정보를 국외 기관(본사, 모회사 또는 계열사, 자회사 및 기타 금융업무 수행을 위해 필요한 관계 기관 포함)으로 이전해야 하는 경우, 다음의 요구 사항을 준수해야 한다.

i) 개인금융정보의 국외 이전은 「개인정보 보호법」 등의 법령과 업계 주관 부서의 관련 규정을 준수해야 한다.

ii) 개인금융정보의 국외 이전은 개인금융정보 주체의 명시적인 동의를 얻어야 한다.

iii) 금융회사는 개인금융정보를 국외로 이전하기 전에 국외 금융기관의 개인정보보호 능력이 중국의 국가, 유관부서 및 금융기관의 보안 요구 사항을 준수할 수 있도록 안전성 평가를 수행해야 한다.

iv) 금융회사는 협약체결 및 현장점검 등을 통해 국외 기관의 개인금융정보 처리 관련 직책 및 의무의 효과적인 이행을 명확히 하고 감독해야 한다.

법률 안내
기업이 금융서비스를 제공하는 경우, 「개인정보 보호법」의 관련 규정을 준수하는 것 외에 다음의 기준도 함께 참고할 것을 권장한다. - 「JR/T 0171-2020 개인금융정보 보호기술 규범」 - 「JR/T 0223-2021 금융데이터보안 - 데이터 수명주기 보안 규범」 - 「JR/T 0197-2020 금융데이터 보안등급 분류 가이드라인」

- 「JR/T 0073-2012 금융업 정보 보안단계 보호 평가 서비스 보안 지침」 - 「GB/T 36629-2018 정보보안기술 - 시민 사이버 전자신원 보안기술 요구 사항」 - 「GB/T 36618-2018 정보보안기술 - 금융정보 서비스 보안 규범」 - 「JR/T 0218-2021 금융업 데이터 역량 강화 지침」

제 6절 의료서비스 제공 시나리오

가. 개인의료정보 범주 및 등급 분류

「GB/T 39725 2020 정보보안기술 - 건강의료 데이터 보안 가이드라인」 제6조에서는 건강 및 의료 데이터를 개인속성 데이터, 건강상태 데이터, 의료응용 데이터, 의료결제 데이터, 건강자원 데이터 및 공중보건 데이터로 구분하고 있다. 개인정보와 연관되는 데이터는 개인속성 데이터, 건강상태 데이터, 의료응용 데이터 및 의료결제 데이터를 포함하며 구체적인 예시는 다음과 같다.

개인정보의 종류	범위
개인속성 데이터	• 인구통계 정보: 성명, 출생일, 성별, 민족, 국적, 직업, 주소, 직장, 가족구성원, 연락처, 소득, 혼인상태 등 • 개인신원 정보: 성명, 신분증, 사원증, 사회보장카드, 건강카드번호, 입원번호 등 • 개인통신 정보: 전화번호, 이메일 주소, 계정 및 관련 정보 • 개인 생체인식 정보: 유전자, 지문, 성문, 손금, 귓바퀴, 홍채, 얼굴특징 등
건강상태 데이터	• 환자서술, 현병력, 과거병력, 가족병력, 신체검사, 가족력, 증상, 검사 데이터, 유전상담 데이터 등
의료응용 데이터	• 외래진료 기록, 입원지시서, 검사보고서, 투약정보, 경과기록, 수술기록, 마취기록, 수혈기록, 간호기록, 입원기록, 퇴원요약, 의뢰(전원)기록, 고지통보정보 등
의료결제 데이터	• 의료거래 정보: 결제정보, 거래금액, 거래기록 등 • 보험정보: 보험상태, 보험금액 등

동시에, 이 가이드라인 제6조는 관련 의료 데이터를 중요도와 위험도에 따라 낮은 정도로부터 높은 정도까지 1~5등급으로 구분하고 있으며, 개인정보보호 사례를 참조하여 다음과 같이 요약하였다.

등급	정의	예시
1등급	공개 채널을 통해 얻을 수 있는 데이터를 포함하여 공개적으로 사용할 수 있는 데이터	
2등급	넓은 범위에서 접근 가능한 데이터	개인정보 주체의 신원을 식별할 수 없는 데이터
3등급	중간 범위에서 접근 가능한 데이터로, 무단으로 공개할 경우 개인정보 주체에게 중간 정도의 피해를 주는 데이터	비식별화 처리하였으나 여전히 재식별 가능한 데이터
4등급	좁은 범위에서 접근 가능한 데이터로, 무단으로 공개할 경우 개인정보 주체에게 비교적 큰 피해를 주는 데이터	신분증번호, 사회보장카드번호 등 직접 개인신원을 식별할 수 있는 정보
5등급	아주 작은 범위에서만 접근 가능한 데이터로, 무단으로 공개할 경우 개인정보 주체에게 중대한 피해를 주는 데이터	특수질환(에이즈, 성병 등) 자료

「GB/T 39725 2020 정보보안기술 - 건강의료 데이터 보안 가이드라인」의 관련 기준에 따라 의료서비스 제공업체는 자사 실정에 따라 위의 가이드라인을 참고하여 처리하는 개인의료정보를 분류할 것을 권장한다.

나. 개인의료정보 수집에 관한 특별 규정

기업이 의료서비스를 제공할 때, 개인의료정보 수집에 관한 특별 요구 사항을 충족하기 위해 「개인정보 보호법」과 관련 법령, 의료산업 법령을 준수해야 한다. 「인구 건강정보 관리 방법(시범시행)」 제8조에 따라 기업은 "일수일원, 최소이용(一數一源, 最少够用)" 원칙에 따라 개인의료정보를 수집해야 한다. 즉, 의료서비스를 제공하는 업체가 수집하는 개인의료정보는 업무상 이용 및 관련 관리 요구 사항을 충족해야 하며 중복수집을 피해야 한다. 상기 원칙에 대한 자세한 내용은 다음과 같다.

① 일수일원 원칙

"일수일원"이란 한 개의 개인정보가 오로지 한 명의 개인정보 주체로부터 얻어지는 것을 의미한다. 의료산업은 여러 사업 분야로 나누어져 있기 때문에 개

인정보 주체 한 명의 개인정보가 여러 곳으로부터 중복수집 될 수 있다. 따라서 중복수집으로 인한 자원 낭비를 줄이고 개인의료정보의 품질을 보장하기 위해, 의료서비스 제공업체는 “일수일원”의 수집 원칙을 준수해야 한다.

② 최소이용 원칙

최소이용 원칙은 「개인정보 보호법」의 필요한 최소한의 원칙과 일맥상통하는 것으로, 의료서비스 제공업체가 처리하는 개인의료정보는 처리목적을 실현하기 위한 최소한의 범위로 제한되어야 하며 개인의료정보를 과도하게 수집하지 말아야 하는 것을 의미한다. 최소이용 원칙의 목적은 개인의료정보의 수집과 보관 비용을 줄이는 한편, 기업의 과도한 개인정보 수집을 방지하려는 데 있다.

다. 개인의료정보 보관에 관한 특별 규정

의료서비스 시나리오에서 기업은 「개인정보 보호법」, 「개인정보안전규범」 및 기타 개인정보 보관에 관한 법적 요구 사항을 준수하는 것 외에도 다음과 같은 특별 규정에 유의해야 한다.

① 계층적 저장, 재해복구 및 백업 요구 사항

「인구 건강정보 관리 방법(시범시행)」 제9조에 따라 의료서비스를 제공하고 개인의료정보를 처리할 때 다음과 같은 조치를 취해야 한다.

i) 기업이 처리하는 개인의료정보는 계층적으로 저장되어야 한다.

ii) 기업은 국가의 관련 규정에 맞는 데이터 저장, 재해복구 및 백업, 관리 조건을 갖추고 신뢰할 수 있는 인구 건강정보 재해복구 및 백업 작업 메커니즘을 구축해야 한다.

iii) 기업은 관련 개인의료정보가 지체 없이 완전하고 정확하게 복원될 수 있도록 정기적으로 백업 및 복원 테스트를 수행해야 한다.

따라서, 의료서비스 제공업체는 「GB/T 39725 2020 정보보안기술 - 건강의료 데이터 보안 가이드라인」과 실제 사업범위에 따라 처리해야 하는 개인의료정보에 대해 범주 및 등급을 분류하여 「인구 건강정보 관리 방법(시범시행)」의 요구사항을 준수할 것을 권장한다.

② 개인정보의 국내 보관에 관한 요구 사항

「인구 건강정보 관리 방법(시범시행)」 제10조 제2항에 따라 인구 건강 관련 개인정보를 국외의 서버에 보관하거나 국외의 서버를 호스팅 또는 임대해서는 아니 된다. 이 규정은 「개인정보 보호법」의 개인정보 보관 기준보다 엄격하므로, 기업은 의료서비스를 제공할 때 「인구 건강정보 관리 방법(시범시행)」 규정을 준수하여 인구 건강 관련 개인정보를 중국 국내에 보관해야 한다.

③ 전자의무기록 봉인

전자의무기록은 환자의 신체 및 건강 상태에 관한 중요한 참고자료로서 환자의 민감 개인정보를 포함하므로 전자의무기록이 분실되는 것을 방지하기 위해 의료서비스 제공업체는 전자의무기록을 봉인할 수 있다. 「전자의무기록 적용 관리 규범(시범시행)」 제5장 (제23조, 제24조, 제25조)의 규정에 따라 환자의 전자의무기록을 봉인하는 경우, 의료서비스 제공업체와 환자(또는 양자의 대리인)가 함께 출석하여 전자의무기록을 확인하고, 복사 및 의무기록 관리도장을 날인한 후 봉인해야 한다.

라. 개인의료정보 접근 및 조회에 대한 특별 규정

개인의료정보는 일반적으로 민감 개인정보에 해당하므로 의료서비스 제공업체는 개인의료정보에 대한 접근 등의 행위에 대해 보다 신중하고 엄격해야 한다. 의료서비스 제공업체는 본 가이드북의 개인정보에 관한 일반 사항 외에 다음과 같은 규정 또는 요구 사항에도 유의해야 한다.

① 「GB/T 39725 2020 정보보안기술 - 건강의료 데이터 보안 가이드라인」 제11.6조에 따르면, 의료서비스 제공업체는 환자의 개인의료정보에 접근하는 경우, 이상행위를 감지할 수 있는 시스템을 구축하여 완전한 접근 경로를 추적할 수 있어야 한다. 더불어, 이상행위가 특정 수준에 이르렀을 때 시스템이 권한잠금 기능을 작동할 수 있어야 한다.

② 「GB/T 39725 2020 정보보안기술 - 건강의료 데이터 보안 가이드라인」 제12.2조에 따르면, 의료서비스 제공업체는 개인의료정보 주체의 계정이 타인에 의해 부정하게 이용되어 정보가 유출되는 것을 방지하기 위해, 개인정보에 대한 조회를 적절하게 제한해야 한다. 예를 들어, HIV, 간염 등의 민감한 검사 결과를 표시하지 않는다던가 3개월 이내의 관련 검사보고서 등의 정보만

조회할 수 있도록 제한해야 한다.

③「전자의무기록 적용 관리 규범(시범시행)」 규정에 따르면, 의료서비스 제공업체는 다음의 요구 사항을 준수해야 한다. 전자의무기록 시스템에 의무기록 열람권한이 설정되어야 하고, 환자의 전자의무기록 자료를 제때에 제공 및 완전하게 표시하여 의료진의 의무기록 열람 수요를 보장해야 한다. 아울러 표시되는 관련 전자의무기록에는 환자 개인정보, 진료기록, 기록 시간 및 담당자, 상급 검토자의 성명 등이 포함되어야 한다. 따라서 의료서비스 제공업체는 전자의무기록 접근에 대한 내부제도를 마련하고, 관련 담당자가 「전자의무기록 적용 관리 규범(시범시행)」에서 요구하는 사항을 쉽게 열람할 수 있도록 명시해야 한다.

마. 개인의료정보 이용에 관한 특별 규정

「개인정보 보호법」의 관련 규정에 따르면, 개인정보를 처리함에 있어 개인정보 주체가 위임한 권한 범위를 벗어날 수 없다. 의료서비스 시나리오에서 기업은 「인구 건강정보 관리 방법(시범시행)」 제14조의 규정에 유의해야 한다. 이 조의 규정에 따라 의료서비스 제공업체는 “인구건강정보 통합 이용 업무 제도”를 구축하고, 관련 개인의료정보에 대한 이용을 승인해야 한다. 따라서, 의료서비스 제공업체는 정보의 통합 이용을 위한 업무 제도와 규범을 마련하고 개인의료정보의 처리 과정에서 해당 제도와 규범을 실행해야 한다.

바. 개인의료정보 주체의 권리행사 대응에 관한 특별 요구 사항

「개인정보 보호법」 제4장의 규정에 따르면, 개인정보 주체는 알 권리, 동의, 열람, 복사, 정정, 보완, 삭제 등의 권리[28]를 갖는다. 그러나 의료서비스를 제공함에 있어 다음과 같이 개인정보 주체의 권리에 대한 특별한 경우와 규정이 있다.

① 개인정보 주체의 권리 약화

의료산업은 종종 공중보건 분야와 관련되는 경우가 있기 때문에 공공의 안전 및 주요 공익에 영향을 미칠 수 있다. 이에 관련 법령에서는 의료산업에서 개인정보 주체의 권리 및 요구 사항에 대해 일정한 제한을 두고 있다. 예를 들어, 「개인정보 보호법」 제13조에 따라 공중보건 사건이 발생하는 경우, 개인정보

28) 개인정보 주체의 권리에 대해서는 본 가이드북 제3장 개인정보 준법 구조의 제3.3절 개인정보 주체의 권리를 참조.

처리자는 관련 개인정보를 직접 처리할 수 있으며, 이는 곧 개인정보 주체의 권리에 대한 약화 행위에 해당한다.

② 개인정보 주체의 조회권

「전자의무기록 적용 관리 규범(시범시행)」 제14조의 규정에 따라 전자의무기록 시스템에는 실무자의 과거 작업 흔적이 온전하게 보관되어야 하고, 작업 시간 및 실무자 정보가 표기되어야 하며, 나아가 이들 실무자의 정보를 조회 및 추적할 수 있어야 한다. 의료서비스를 제공함에 있어 많은 양의 개인의료정보가 전자의무기록 시스템에 기록된다. 따라서, 개인정보 주체의 충분한 조회권을 보장하기 위해, 실무자가 개인의료정보를 처리할 수 있는 제도와 규범을 마련하고 정기적으로 작업일지를 기록해야 한다.

유의 사항
기업이 의료서비스를 제공하는 경우, 「개인정보 보호법」의 관련 규정을 준수하는 것 외에 다음의 법규도 함께 참고할 것을 권장한다. - 「GB/T 39725 2020 정보보안기술 - 건강의료 데이터 보안 가이드라인」 - 「인구 건강정보 관리 방법(시범시행)」 - 「전자의무기록 적용 관리 규범(시범시행)」 - 「국가 건강의료 빅데이터 표준, 보안 및 서비스 관리 방법」 - 「온라인 진료 관리방법(시범시행)」 - 「원격 의료 서비스 관리규범(시범시행)」 - 「전자의무기록 시스템 적용 수준 차등평가 관리 방법(시범시행)」 - 「의약품 임상시험 품질관리 규범」

제 7절 직원 개인정보 국외 이전 시나리오

가. 직원 개인정보의 정의

「개인정보 보호법」, 노동법 및 관련 규정에 따라 직원 개인정보는 기업의 직원 관련 전자적 또는 기타 방식으로 기록된 이미 식별되거나 식별 가능한 다양한 정보를 뜻하며 직원 성명, 성별, 출생일, 신분증번호, 생체정보, 주소, 전화번호 등을 포함하되 이에 국한되지 아니한다. 따라서 기업이 노동 및 인사 관리 과정에서 취득한 직원 개인이력서, 면접정보, 배경조사보고서, 신체검사보고서, 개인정보기록 서류, 지문 또는 얼굴, 급여수준, 위치정보 등은 모두 개인정보의 범주에 해당한다.

나. 직원 개인정보의 국외 이전 시나리오

「개인정보 보호법」에 따른 개인정보의 국외 이전에 관한 규정에 따라 다음과 같은 상황은 모두 직원 개인정보의 국외 이전에 해당한다고 사료된다.

- 다국적 기업이 글로벌 경영을 위해 직원 개인정보를 해외 본사로 전송하는 경우
- 다국적 기업이 인적자원관리 IT 시스템의 서버를 국외에 구축하거나 서버가 중국 국내에 구축되었더라도 해외 본사에 접근 경로를 제공하는 경우

다. 기업 직원 개인정보의 국외 이전에 관한 특별 요구 사항

① 특정 기업의 직원 개인정보 국외 이전에 관한 특별 요구 사항

「개인정보 보호법」 제40조에 따라 ① 핵심정보인프라시설 운영자에 의해 수집 및 생성된 개인정보 및 ② 개인정보의 국외 이전이 일정량에 달한 활동의 경우, 관련 기업의 직원 개인정보를 포함한 개인정보는 중국 내에 보관하는 것을 원칙으로 한다. 만약 관련 기업이 필히 직원의 개인정보를 국외로 이전해야 하는 경우라면, 국가네트워크정보 당국에서 주관하는 안전성 평가를 통과해야 한다[29].

② 기업 직원 개인정보의 국외 이전에 관한 일반 요구 사항

i)「개인정보 보호법」에서 규정하는 개인정보의 국외 이전을 허용하는 법적 요건

일반 기업이 직원 개인정보를 국외로 이전해야 하는 경우, 「개인정보 보호법」 제38조의 규정에 따라 적어도 아래 법적 요구 사항 중 하나를 충족해야 한다.

- 국가네트워크정보 당국에서 주관하는 안전성 평가를 통과해야 한다.

29) 일반 개인정보의 국외 이전에 관한 내용은 본 가이드북 제3장 개인정보 준법 구조의 제3.6절 개인정보의 국외 이전 중 제2항 개인정보의 국외 이전에 관한 기본 규칙을 참조.

- 국가네트워크정보 당국의 규정에 따라 전문 기관으로부터 개인정보보호 인증을 실시해야 한다.
- 국가네트워크정보 당국에서 정한 표준계약에 따라 국외의 이전 받는 자와 계약을 체결하고 양자의 권리와 의무를 명확하게 약정해야 한다.
- 법률, 행정법규 또는 국가네트워크정보 당국에서 정한 기타 조건.

ii) 고지사항 및 별도의 동의

「개인정보 보호법」 제39조에 따르면, 기업이 개인정보를 국외로 이전하는 경우, 개인정보의 국외 이전을 고지하고 별도의 동의를 얻어야 한다.

기업이 「개인정보 보호법」 제13조의 5가지 적법성에 따라 개인정보 처리에 관한 개인정보 주체의 동의가 필요 없는 경우라 하더라도 개인정보 국외이전에 관한 동의까지 면제받을 수 없다는 견해가 많다.

따라서 기업은 개인정보의 국외 이전에 관한 국가 입법 당국의 입법 동향과 법집행 당국의 태도에 유의할 필요가 있다. 아울러, 실무상 기업이 직원의 개인정보를 국외로 이전해야 하는 경우, 사내 시스템 팝업창, 이메일 및 종이문서 등의 방식으로 관련 직원에게 알려 별도의 동의를 취득함으로써 “일반 공고” 등의 “패키지” 방식으로 승인을 얻는 것을 방지해야 한다.

iii) 직원 개인정보 국외 처리 시의 상호주의 원칙

첫째, 기업은 「개인정보 보호법」 제38조에 따라 국외에서 개인정보를 이전 받는 자가 직원의 개인정보를 처리함에 있어 관련 활동이 「개인정보 보호법」에서 요구하는 개인정보보호 기준을 충족할 수 있도록 필요한 조치를 취해야 한다.

둘째, 「개인정보 보호법」 제43조는 정보의 국외 이전에 대한 “상호주의 원칙”을 규정하고 있다. 즉, 개인정보보호 면에 있어 정보를 이전 받는 국가 또는 지역이 중국에 대해 차별적인 금지, 제한 또는 기타 유사한 조치를 취할 경우, 중국은 실제 상황에 따라 해당 국가 또는 지역에 대해 대등한 조치를 취한다.

따라서 기업이 직원의 개인정보를 국외로 이전해야 하는 경우, 향후 국외 이전에 대해 앞서 언급한 상호주의 원칙에 의한 잠재적 위험성을 고려하여 실제 상황에 따라 직원의 개인정보를 국외로 이전할지 여부를 결정해야 한다.

유의 사항
기업이 직원의 개인정보를 국외로 이전하는 경우 다음과 같은 조치를 취할 것을 권장한다. - 개인정보의 국외 이전에 대해 사전에 직원의 동의 또는 별도의 동의를 얻는 활

동을 통해 기업의 개인정보보호제도를 개선한다.
- 기업의 취업규칙 및 기타 제도에 직원 개인정보보호에 관한 장(chapter)을 추가하여 직원 개인정보에 대한 기업의 관리원칙과 국외 이전 관련 규정을 명시한다.
- 직원의 개인정보 관련 서류를 선별하고, 국외로 이전하는 직원의 개인정보에 대해 기술적 보호 조치를 취한다.
- 국외의 이전 받는 자와 국내 직원의 개인정보 처리 계약을 체결하고 양자의 권리와 의무를 명확하게 약정하며, 국외에서 직원 개인정보를 이전 받는 자의 개인정보 처리활동이 중국의 관련 법령에서 정한 기준을 충족하는지 감독한다.
- 직원의 개인정보를 국외로 이전하기 전에 위험성 및 보호조치에 대한 평가를 실시하고 분석보고서를 작성하여 보관해야 한다.
- 기업의 직원 개인정보를 국외로 이전할 필요가 없는 경우, 중국 현지에서 서버를 구축하여 보관하는 것을 고려해볼 수 있다.
- 개인정보의 국외 이전에 관한 내용을 구체화 하는 법령이 제정될 것으로 예상되므로 법령 동향을 꾸준히 모니터링 할 필요가 있다.

법규 안내

기업이 직원의 개인정보를 국외로 이전할 때, 「개인정보 보호법」의 관련 규정을 준수하는 것 외에 다음의 기준도 함께 참고할 것을 권장한다.
- 「개인정보안전규범」
- 「개인정보 및 중요 데이터 국외 이전 보안평가 방법(의견수렴안)」
- 「개인정보 국외 이전 보안평가 방법(의견수렴안)」
- 「정보보안기술 - 데이터 국외 이전 보안평가 지침(의견수렴안)」
- 「데이터 국외 이전 보안평가 방법(의견수렴안)」

개인정보의 국외 이전에 관한 법령이 아직 제정 중인 상황에서 개인정보의 국외 이전에 관한 입법 동향에 항상 주의를 기울이고, 기업이 속한 업계 및 경영상황에 따라 직원 개인정보의 국외 이전에 대한 내부 제도 및 규범을 조정해야 한다.

제 5장 단계별 규정 준수

기업이 개인정보보호 관련 준법 활동을 수행할 때 「개인정보 보호법」 및 관련 법령을 근거로 하여 관련 기술표준을 도입하는 동시에, 아래에 안내하는 절차와 운영방법을 참고하여 완전한 개인정보보호 준법 시스템을 구축해야 한다.

제 1절 현황 점검

자체 개인정보보호 현황을 점검(실사)하고 보고서를 작성해야 하며, 점검 내용은 다음 사항을 포함하되 이에 국한되지 아니한다.
가. 개인정보의 수집 및 이용, 공유, 보관, 삭제 등 개인정보 처리활동의 전 수명 주기 차원에서 제품 또는 서비스의 개인정보 처리 상황을 분석하고, 개인정보의 수집 종류, 흐름, 구체적인 적용 시나리오, 범주 및 등급 분류 상황, 개인정보보호에 있어 기업의 역할 및 이미 취한 안전상 보호조치 등을 검토한다.
나. 제품 또는 서비스가 제3자로부터 개인정보를 구매하는 행위와 연관되는지 및 제3자 협력사(제3자 서비스 제공자, 공급업체 등 포함)와의 개인정보 공유 및 협력 시나리오에서의 개인정보 처리활동, 권리 및 의무 분담 상황을 파악한다.
다. 제품 또는 서비스의 등록 약정, 개인정보보호정책, 인터페이스 디자인, 개인정보보호 설정, 이용자 권리 대응 프로세스, 각 제품 라인의 승인 방식 및 범위, 관리 메커니즘 등의 제도적 규범, 문서 및 계약을 검토한다.
라. 업무 절차, 내부 권한 할당, 기술적 보호조치, 기술적 운영 규범 및 기타 관리, 기술적 조치를 포함한 기업의 현행 개인정보보호제도를 파악한다.

제 2절 격차 분석

「개인정보 보호법」 및 관련 법령, 규제 동향에 따라 앞서 언급한 자체 점검 결과에 따라 기업의 개인정보보호제도 및 제품 또는 서비스 등 면에서 잠재적인 준법 리스크를 분석해야 하며, 이에는 다음 내용을 포함하되 이에 국한되지 아니한다.

가. 기업의 개인정보보호제도 측면

① 사내 개인정보보호제도 구축 상황. 예를 들어, 법에서 요구하는 관련 개인정보보호제도가 미비하거나 불완전한지 여부, 개인정보보호 관리부서 또는 전담인력을 확보하였는지 여부 등

② 사내 개인정보 처리활동에 대한 위험 분석. 예를 들어, 기업의 개인정보 접근제도에서 접근권한에 대한 제한이 적절한지 여부, 기업에서 수집한 개인정보가 수집 당시 고지한 용도 이외의 다른 용도로 사용되는지 여부 등

나. 제품 또는 서비스 측면

① 제품 또는 서비스의 개인정보 처리활동에 대한 위험성 분석. 예를 들어, 개인정보 처리활동에 대한 법적 근거가 있는지 여부, 제품 또는 서비스 제공 과정에서 개인정보가 과도하게 수집되는지 여부 등

② 이용자를 대상으로 한 제품 또는 서비스의 「개인정보보호정책」, 「서비스 이용약관」 등 문서에 대한 위험성 종합 분석. 예를 들어, 「개인정보보호정책」이 개인정보 수집 목적 및 범위를 이용자에게 고지하는지 여부, 「서비스 이용약관」이 개인정보 주체의 권리행사 상황, 방법 및 대응 방법을 명시하는지 여부 등

③ 제품 또는 서비스 관련 제3자 협력사(제3자 서비스 제공자, 공급업체 등 포함)와 체결한 협력계약의 핵심 조항에 대한 위험성 파악. 예를 들어, 해당 협력계약에서 양자의 권리와 의무가 분명한지, 개인정보의 처리를 위탁하는 자가 위임받는 자의 개인정보 처리를 감독하는 메커니즘 및 방법을 규정하는지 여부.

위의 분석을 바탕으로 다음과 같은 조치를 취할 수 있다.

i) 개인정보 처리 시나리오별 위험도를 높음, 보통, 낮음 3단계로 구분하여 표시하고 격차분석표(실사보고서)를 작성한다.

ii) 업무 책임자 및 법집행 기관과 충분히 소통하고 준법 건의사항을 제시하여 준법건의서를 작성한다.

iii) 업무의 긴급성 및 중요성에 따라 시정계획서를 작성한다.

제 3절 준법 이행

앞서 언급한 격차분석표 및 시정계획서를 기반으로 업무상 필요 및 실제 상황에 따라 구체적인 개인정보보호제도 시행계획을 수립한다. 이에는 다음을 포함하되 이에 국한되지 아니한다.

가. 기업의 개인정보보호제도 측면

① 기업의 개인정보보호 관련 강령성 문서를 정하고 그 강령을 실현하기 위한 업무구조 및 기본적인 제도를 수립한다.

② 개인정보보호 전문 기구를 설립하거나 개인정보보호책임자를 선임하여 개인정보보호 업무를 견인하고 사내 각 부서의 개인정보보호업무를 총괄하도록 한다.

③ 개인정보 범주 및 등급 분류, 개인정보 보관 및 파기, 개인정보 영향평가, 제3자 개인정보 준법관리(고객, 협력사, 공급업체 등 포함), 개인정보 보안사건 비상대책 등을 포함하는 개인정보보호업무 관련 내부 규범을 마련한다.

나. 제품 또는 서비스 측면

① 제품 또는 서비스에 대한 「개인정보보호정책」 및 이용약관을 최적화한다.

② 개인정보 주체가 권리행사 시 이용하는 인터페이스 및 경로 설정을 최적화한다.

③ 제3자와의 협력계약을 법규에 부합하는 내용으로 최적화하고 제3자 주체가 고객인지 데이터 소스인지, 개인정보 처리 관계가 공유인지 위탁처리인지 등을 포함하여 다양한 개인정보 처리 관계에 따라 각기 다른 협력계약 양식을 정한다.

제 4절 지속적인 개선

기업은 법령에서 요구하는 완전한 개인정보보호제도를 구축한 후, 장기적이고 정기적인 교육 및 검사 활동을 수행해야 한다. 아울러, 기업은 갱신된 법령 및 관련 기술 표준과 업무상 수요에 따라 개인정보보호제도를 조정하고 최적화하여 개인정보보호수준을 지속적으로 향상시켜야 한다. 이를 위해, 다음과 같은 조치를 취할 수 있다.

가. 지속적으로 교육 활동 실시 : 실제 수요에 따라 다양한 그룹을 대상으로 교육 활동을 전개할 수 있다. 예컨대 경영진, 주요 업무라인의 핵심인력, 법무 및 전 직원을 상대로 단계별 맞춤형 교육을 실시하여 직원별 개인정보보호에 대한 준법 인식을 꾸준히 제고할 수 있다. 교육방법에는 강의실 교육, 온라인 학습, 포스터 활동, 홍보책자 및 세미나 등을 포함하지만 이에 국한되지 아니한다.

나. 정기적인 준법감사 실시 : 준법감사는 기업이 자체 개인정보보호시스템의 운영실태를 평가하는데 도움될 수 있다.

다. 업계 모범 사례 및 입법, 법집행, 사법동향 예의주시 : 업계의 「개인정보 보호법」 실행 상황을 예의주시하고, 개인정보보호 관련 입법, 법집행 및 사법동향에 세심한 주의를 기울이며, 기업의 개인정보보호 제도 및 절차를 제때에 조정하여 관련 준법의무를 이행해야 한다.

제 6장 「개인정보 보호법」 및 관련 법령

이 장에서는 개인정보보호 관련 법령체계를 열거하여 개인정보보호 법률체계의 논리적 틀과 구조를 명확히 한다.

순번	파일명	공포기관	발효일
법률 및 관련 법률 이슈에 대한 해석			
1	「중화인민공화국 개인정보 보호법」	전국인민대표대회 상무위원회	2021년 11월 1일
2	「중화인민공화국 데이터 보안법」	전국인민대표대회 상무위원회	2021년 9월 1일
3	「중화인민공화국 미성년자보호법」	전국인민대표대회 상무위원회	2021년 6월 1일
4	「중화인민공화국 도로교통안전법」	전국인민대표대회 상무위원회	2021년 4월 29일
5	「중화인민공화국 민법전」	전국인민대표대회	2021년 1월 1일
6	「중화인민공화국 전자상거래법」	전국인민대표대회 상무위원회	2019년 1월 1일
7	「중화인민공화국 사이버 보안법」	전국인민대표대회 상무위원회	2017년 6월 1일
8	「중화인민공화국 형법 개정안(9)」	전국인민대표대회 상무위원회	2015년 11월 1일
9	「중화인민공화국 소비자권익보호법」	전국인민대표대회 상무위원회	2014년 3월 15일
10	「인터넷 정보 보호 강화에 관한 전국인민대표대회 상무위원회 결정」	전국인민대표대회 상무위원회	2012년 12월 28일
11	「중화인민공화국 형법 개정안(7)」	전국인민대표대회 상무위원회	2009년 2월 28일
행정법규			
1	「핵심정보인프라시설 보안 보호 조례」	국무원	2021년 9월 1일
2	「중화인민공화국 인류유전자원 관리조례」	국무원	2019년 7월 1일
3	「인터넷 서비스 영업장 관리조례」	국무원	2019년 3월 24일

4	「중화인민공화국 전기통신 조례」	국무원	2016년 2월 6일
5	「지도관리조례」	국무원	2016년 1월 1일
6	「신용조사업 관리조례」	국무원	2013년 3월 15일
7	「컴퓨터 정보 시스템 안전보호 조례」	국무원	2011년 1월 8일
사법 해석			
1	「안면인식 기술을 이용한 개인정보 처리 관련 민사사건을 심리하는데 있어 약간의 법률 적용 쟁점에 관한 최고인민법원의 규정」	최고인민법원	2021년 8월 1일
2	「정보망을 이용한 개인 권익침해 관련 민사분쟁 사건을 심리하는 데 있어 약간의 법률 적용 문제에 관한 최고인민법원의 규정」	최고인민법원	2021년 1월 1일
3	「정보망 불법 사용 및 정보망 범죄 활동 지원 등의 형사사건 처리에 있어 약간의 법률 적용 문제에 관한 최고인민법원 및 최고인민검찰원의 해석」	최고인민법원, 최고인민검찰원	2019년 11월 1일
4	「시민 개인정보 침해에 관한 형사사건 심판에 있어 약간의 법률 적용 쟁점에 관한 최고인민법원 및 최고인민검찰원의 해석」	최고인민법원, 최고인민검찰원	2017년 6월 1일
부서별 규정 및 규범성 문서			
1	「신용조사업무 관리 방법」	중국인민은행	2022년 1월 1일
2	「차량 데이터 보안에 관한 약간의 규정(시범시행)」	국가네트워크정보국, 중화인민공화국 국가발전개혁위원회, 중화인민공화국 공업정보화부,	2021년 10월 1일

		중화인민공화국 공안부, 중화인민공화국 교통운수부	
3	「사물인터넷 기본 보안표준 시스템 구축 가이드라인(2021년판)」	공업정보화부	2021년 9월 23일
4	「인터넷 정보 서비스 알고리즘 통합 거버넌스 강화에 관한 지도 의견」	국가네트워크정보국, 중국공산당 중앙선전부, 교육부, 과학기술부, 공업정보화부, 공안부, 문화여행부, 국가시장감독관리총국, 국가라디오방송총국	2021년 9월 17일
5	「지능형 커넥티드 차량 일반도로 시범운행 및 시범응용 관리 규범(시범시행)」	공업정보화부, 공안부, 교통운수부	2021년 9월 1일
6	「네트워크 제품 보안 취약점 관리 규정」	공업정보화부, 국가네트워크정보국, 공안부	2021년 9월 1일
7	「금융기관의 자금세탁 방지 및 테러 자금조달 방지 관리감독 방법」	중국인민은행	2021년 8월 1일
8	「지능형 커넥티드 차량 제조사 및 제품 진입 관리 강화에 관한 공업정보화부의 의견」	공업정보화부	2021년 7월 30일
9	「인터넷 생중계 마케팅 관리 방법(시범시행)」	국가네트워크정보국, 공안부, 상무부, 문화여행부, 국가세무총국, 국가시장감독관리총국, 국가라디오방송총국	2021년 5월 25일
10	「일반 유형의 모바일 인터넷 앱에 필요한 개인정보 범위에 관한 규정」	국가네트워크정보국, 공업정보화부, 공안부, 국가시장감독관리총국	2021년 5월 1일
11	「네트워크 거래 관리감독 방법」	국가시장감독관리총국	2021년 5월 1일
12	「인터넷 이용자 공식 계정 정보 서비스 관리 규정」	국가네트워크정보국	2021년 2월 22일
13	「인터넷 생중계 표준화 관리 업무 강화에 관한 지도 의견」	국가네트워크정보국, 전국 “음란 및 불법 출판물 단속” 실	2021년 2월 9일

		무그룹 판공실, 공업정보화부, 공안부, 문화여행부, 국가시장감독관리총국, 국가라디오방송총국	
14	「중국인민은행 금융소비자 권익보호 시행 조치」	중국인민은행	2020년 11월 1일
15	「소비자 권익침해행위 처벌 방법」	국가공상행정관리총국	2020년 10월 23일
16	「의약품 임상시험 품질관리 규범」	국가의약품감독관리국, 국가위생건강위원회	2020년 7월 1일
17	「사이버 보안 심사 방법」	국가네트워크정보국, 국가발전개혁위원회, 공업정보화부, 공안부, 국가안전부, 재정부, 상무부, 중국인민은행, 국가시장감독관리총국, 국가라디오방송총국, 국가기밀국, 국가암호관리국	2020년 6월 1일
18	「사이버 정보 콘텐츠 생태계 거버넌스 규정」	국가네트워크정보국	2020년 3월 1일
19	「산업데이터 범주 및 등급 분류 가이드라인(시범시행)」	공업정보화부	2020년 2월 27일
20	「네트워크 오디오 및 비디오 정보 서비스 관리 규정」	국가네트워크정보국, 문화여행부, 국가라디오방송총국	2020년 1월 1일
21	「APP에 의한 개인정보 무단 수집 및 이용 행위 판정 방법」	국가네트워크정보국, 공업정보화부, 공안부, 국가시장감독관리총국	2019년 11월 28일
22	「온라인 아동 개인정보보호 규정」	국가네트워크정보국	2019년 10월 1일
23	「클라우드 컴퓨팅 서비스 보안평가 방법」	국가네트워크정보국, 국가발전개혁위원회, 공업정보화부, 재정부	2019년 9월 1일
24	「인터넷 개인정보보안 보호 지침」	공안부, 베이징인터넷산업협회	2019년 4월 10일

25	「APP에 의한 개인정보 무단 수집 및 이용에 대한 자가진단 지침」	App을 통한 개인정보 무단 수집 및 이용 특별 거버넌스 실무그룹	2019년 3월 3일
26	「전자의무기록 시스템 적용 수준 차등평가 관리 방법(시범시행)」	국가위생건강위원회	2018년 12월 3일
27	「여론적 속성 또는 사회적 동원 능력이 있는 인터넷 정보 서비스 안전성 평가 규정」	국가네트워크정보국, 공안부	2018년 11월 30일
28	「온라인 진료 관리방법(시범시행)」	국가위생건강위원회, 국가중의약관리국	2018년 9월 28일
29	「원격 의료 서비스 관리규범(시범시행)」	국가위생건강위원회, 국가중의약관리국	2018년 7월 17일
30	「국가 건강의료 빅데이터 표준, 보안 및 서비스 관리 방법(시범시행)」	국가위생건강위원회	2018년 7월 12일
31	「전자의무기록 적용 관리 규범(시범시행)」	국가위생 및 계획생육위원회, 국가중의약관리국	2017년 4월 1일
32	「인터넷 광고 관리 잠정 조치」	국가공상행정관리총국	2016년 9월 1일
33	「인구 건강정보 관리 방법(시범시행)」	국가위생 및 계획생육위원회	2014년 5월 5일
34	「전기통신 및 인터넷 이용자 개인정보보호 규정」	공업정보화부	2013년 9월 1일
35	「인터넷 정보 서비스 시장질서 규제에 관한 약간의 규정」	공업정보화부	2012년 3월 15일
36	「금융기관 고객신원식별, 고객신원 자료 및 거래기록 보관관리 방법」	중국인민은행, 중국은행감독관리위원회, 중국증권감독관리위원회, 중국보험감독관리위원회	2007년 8월 1일
37	「데이터 국외 이전 보안평가 방법(의견수렴안)」	국가네트워크정보국	의견수렴안(2021년 10월 29일 공포)
38	「산업 및 정보화 분야 데이터 보안관리 방법(시범시행)(의견수렴안)」	공업정보화부	의견수렴안(2021년 9월 30일 공포)

39	「인터넷 정보 서비스 알고리즘 추천 관리 규정(의견수렴안)」	국가네트워크정보국	의견수렴안 (2021년 8월 27일 공포)
40	「차량인터넷(지능형 커넥티드 차량) 네트워크안전 업무 강화에 관한 통지 (의견수렴안)」	공업정보화부	의견수렴안 (2021년 6월 22일 공포)
41	「차량인터넷(지능형 커넥티드 차량) 네트워크안전 표준 시스템 구축 가이드라인(의견수렴안)」	공업정보화부	의견수렴안 (2021년 6월 21일 공포)
42	「모바일 인터넷 앱 개인정보보호 관리 잠정 규정(의견수렴안)」	공업정보화부	의견수렴안 (2021년 4월 26일 공포)
43	「비은행 결제기관 조례(의견수렴안)」	중국인민은행	의견수렴안 (2021년 1월 20일 공포)
44	「개인정보 국외 이전 보안평가 방법 (의견수렴안)」	국가네트워크정보국	의견수렴안 (2019년 6월 13일 공포)
45	「데이터 보안 관리 방법(의견수렴안)」	국가네트워크정보국	의견수렴안 (2019년 5월 28일 공포)
46	「사이버 보안 단계 보호 조례(의견수렴안)」	공안부	의견수렴안 (2018년 6월 27일 공포)
47	「개인정보 및 중요 데이터 국외 이전 보안평가 방법(의견수렴안)」	국가네트워크정보국	의견수렴안 (2017년 4월 11일 공포)
국가 산업 표준			
1	「차량 수집 데이터 처리 보안 가이드라인」(TC260-001)	전국정보보안표준화기술위원회	2021년 10월 8일
2	「네트워크 핵심장비 보안 일반 요구사항」(GB 40050-2021)	국가시장감독관리총국, 중국국가표준화관리위원회	2021년 8월 1일
3	「정보보안기술 - 건강의료 데이터 보안 가이드라인」(GB/T 39725-2020)	국가시장감독관리총국, 중국국가표준화관리위원회	2021년 7월 1일

4	「정보보안기술 - 개인정보 보안 영향평가 지침」(GB/T 39335-2020)	국가시장감독관리총국, 중국국가표준화관리위원회	2021년 6월 1일
5	「금융데이터보안 - 데이터 수명주기 보안 규범」(JR/T 0223-2021)	중국인민은행	2021년 4월 8일
6	「인공지능 알고리즘 금융 적용 평가 규범」(JR/T 0221-2021)	중국인민은행	2021년 3월 26일
7	「금융업 데이터 역량 강화 지침」(JR/T 0218-2021)	중국인민은행	2021년 2월 9일
8	「사이버 보안 표준 실무 지침 - 인공지능의 윤리적 보안 위험 예방 가이드라인」(TC260-PG-20211A)	전국정보보안표준화기술위원회	2021년 1월 5일
9	「사이버 보안 표준 실무 지침 - 모바일 인터넷 앱(App)의 소프트웨어 개발 키트(SDK) 사용 관련 보안 가이드라인」(TC260-PG-20205A)	전국정보보안표준화기술위원회	2020년 11월 27일
10	「정보보안기술 - 원격 안면인식 시스템 기술 요구 사항」(GB/T 38671-2020)	국가시장감독관리총국, 중국국가표준화관리위원회	2020년 11월 1일
11	「정보보안기술 - 사이버 보안 단계 보호를 위한 단계화 지침」(GBT 22240-2020)	국가시장감독관리총국, 중국국가표준화관리위원회	2020년 11월 1일
12	「정보보안기술 - 개인정보 보안 규범」(개인정보안전규범)(GB/T 35273-2020)	국가시장감독관리총국, 중국국가표준화관리위원회	2020년 10월 1일
13	「정보보안기술 - 생체인식 기반 모바일 스마트 단말기 신원인증 기술 프레임워크」(GB／T 38542-2020)	국가시장감독관리총국, 중국국가표준화관리위원회	2020년 10월 1일
14	「차량인터넷 정보 서비스 - 데이터 보안 기술 요구 사항」(YD/T 3751-2020)	공업정보화부	2020년 10월 1일
15	「차량인터넷 정보 서비스 - 이용자	공업정보화부	2020년

	개인정보보호 요구 사항」(YD/T 3746-2020)		10월 1일
16	「금융데이터보안 - 데이터 보안 분류 지침」(JR/T 0197－2020)	중국인민은행	2020년 9월 23일
17	「사이버 보안 표준 실무 지침 - 모바일 인터넷 앱(App)의 시스템 권한 신청 사용 지침」(TC260-PG-20204A)	전국정보보안표준화기술위원회	2020년 9월 18일
18	「사이버 보안 표준 실무 지침 - 모바일 인터넷 앱(App) 개인정보보호 관련 자주 묻는 질문 및 처리 지침」(TC260-PG-20203A)	전국정보보안표준화기술위원회	2020년 9월 18일
19	「사이버 보안 표준 실무 지침 - 모바일 인터넷 앱(App) 개인정보 수집 및 이용 자가진단 가이드라인」(TC260-PG-20202A)	전국정보보안표준화기술위원회	2020년 7월 22일
20	「정보보안기술 - 사이버 보안 단계 보호 시행 지침」(GBT 25058-2019)	국가시장감독관리총국, 중국국가표준화관리위원회	2020년 3월 1일
21	「정보보안기술 - 개인정보 비식별화 처리 지침」(GB/T 37964-2019)	국가시장감독관리총국, 중국국가표준화관리위원회	2020년 3월 1일
22	「정보보안기술 - 데이터 보안 기능 성숙도 모델」(GB／T 37988-2019)	국가시장감독관리총국, 중국국가표준화관리위원회	2020년 3월 1일
23	「정보보안기술 - 데이터 거래 서비스 보안 요구 사항」(GB／T 37932-2019)	국가시장감독관리총국, 중국국가표준화관리위원회	2020년 3월 1일
24	「개인 금융정보 보호기술 규범」(JR/T 0171-2020)	중국인민은행	2020년 2월 13일
25	「정보보안기술 - 사이버 보안 단계 보호 기준」(GBT 22239-2019)	국가시장감독관리총국, 중국국가표준화관리위원회	2019년 12월 1일
26	「정보보안기술 - 사이버 보안 단계 보호를 위한 보안설계의 기술적 요구	국가시장감독관리총국, 중국국가표준화관리위원회	2019년 12월 1일

	사항」(GBT 25070-2019)		
27	「정보보안기술 - 사이버 보안 단계 보호를 위한 평가 요구 사항」(GBT 28448-2019)	국가시장감독관리총국, 중국국가표준화관리위원회	2019년 12월 1일
28	「정보보안기술 - 사물인터넷 보안 참조 모델 및 일반 요구 사항」(GB/T 37044-2018)	국가시장감독관리총국, 국가표준화관리위원회	2019년 7월 1일
29	「정보보안기술 - 사물인터넷 데이터 전송 보안 기술 요구 사항」(GB/T 37025-2018)	국가시장감독관리총국, 국가표준화관리위원회	2019년 7월 1일
30	정보보안기술 - 사물인터넷 감지계층 게이트웨이 보안기술 요구 사항」(GB/T 37024-2018)	국가시장감독관리총국, 국가표준화관리위원회	2019년 7월 1일
31	「정보보안기술 - 사물인터넷 감지계층 통신망 연결 보안 요구 사항」(GB/T 37093-20)		
32	「사이버 보안 실무 지침 - 모바일 인터넷 앱의 기본 업무 기능을 위한 필수 정보 사양」	전국정보보안표준화기술위원회	2019년 6월 1일
33	「정보보안기술 - 시민 사이버 전자 신원 보안기술 요구 사항」(GB/T 36629-2018)	국가시장감독관리총국, 중국국가표준화관리위원회	2019년 5월 1일
34	「정보보안기술 - 금융정보 서비스 보안 규범」(GB/T 36618-2018)	국가시장감독관리총국, 중국국가표준화관리위원회	2019년 4월 1일
35	「정보보안기술 - 모바일 스마트 단말기 개인정보보호 기술 요구 사항」(GB/T 34978-2017)	중화인민공화국 국가품질감독검사검역총국, 중국국가표준화관리위원회	2018년 5월 1일
36	「금융업 정보 보안단계 보호 평가 서비스 보안 지침」(JR/T 0073-2012)	중국인민은행	2012년 7월 6일
37	「정보보안기술 - 차량 수집 데이터의 보안 요구 사항(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2021년 10월 19일 공포)
38	「사이버 보안 표준 실무 지침 - 데	전국정보보안표준화기술위원	의견수렴안

	이터 범주 및 등급 분류 지침(의견수렴안)」	회	(2021년 9월 30일 공포)
39	「인터넷 의료건강 정보보안 관리 규범(의견수렴안)」	중화인민공화국 국가위생건강위원회	의견수렴안 (2021년 6월 3일 공포)
40	「정보보안기술 - 커넥티드 차량 - 수집 데이터의 보안 요구 사항(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2021년 4월 28일 공포)
41	「정보보안기술 - 안면인식 데이터 보안 요구 사항(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2021년 4월 23일 공포)
42	「정보보안기술 - 모바일 인터넷 앱(APP) SDK 보안 지침(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2021년 4월 19일 공포)
43	「정보보안기술 - 모바일 인터넷 앱(APP) 개인정보 보안평가 규범(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2021년 4월 19일 공포)
44	「정보보안기술 - 개인정보 비식별화 효과 등급 구분 평가 규범(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2021년 4월 12일 공포)
45	「정보보안기술 - 네트워크 오디오 및 비디오 서비스 데이터 보안 지침(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2021년 2월 24일 공포)
46	「정보보안기술 - 인터넷 결제 서비스 데이터 보안 지침(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2021년 2월 24일 공포)
47	「정보보안기술 - 온라인 쇼핑 서비스 데이터 보안 지침(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2021년 2월 24일 공포)
48	「정보보안기술 - 정보 보안사건 범주 및 등급 분류 지침(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2021년 1월 22일 공포)
49	「정보보안기술 - 사이버 데이터 처리 보안 규범(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2020년 8월 28일 공포)
50	「정보기술 - 보안기술 - 개인식별	전국정보보안표준화기술위원	의견수렴안

	가능한 정보(PII) 처리자에 의한 공용 클라우드의 PII 보호 실행 지침(의견수렴안)」	회	(2020년 7월 15일 공포)
51	「사이버 보안 표준 실무 지침 - 모바일 인터넷 앱(App) 개인정보 보안 지침(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2020년 3월 30일 공포)
52	「정보보안기술 - 모바일 인터넷 앱(App) 개인정보 수집 기본 규범(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2020년 1월 20일 공포)
53	「정보보안기술 - 개인정보 고지 및 동의 가이드라인(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2020년 1월 20일 공포)
54	「정보기술 - 보안기술 - 생체정보 보호 요구 사항 (의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2019년 6월 25일 공포)
55	「정보보안기술 - 데이터 국외 이전 보안평가 지침(의견수렴안)」	전국정보보안표준화기술위원회	의견수렴안 (2017년 8월 30일 공포)

청렴韓세상

윤리경영·청렴 레터

KOTRA에 대해 관심과 지원을 해주신 귀하(사)에
진심으로 감사의 말씀을 드립니다.
KOTRA는 윤리경영·청렴을 통해 투명하고, 공정하고 책임있게
업무를 수행함으로써 고객 여러분께 수준 높은 서비스를 제공하기 위하여
다음과 같은 사항을 실천해 나가고 있습니다.

첫째, 긍지와 자부심을 가지고 명예와 자존심을 소중히 여기며 깨끗하고 투명한 공직사회 건설에 앞장선다.

둘째, 행동강령에 어긋나는 금품·향응을 거부하고, 외부로부터의 어떠한 압력과 청탁도 배격한다.

셋째, 직위를 이용하여 부당한 이익을 추구하지 않으며, 성실하고 공정하게 맡은 바 업무를 수행한다.

넷째, 항상 사람을 최우선하고, 임직원, 고객, 협력사, 유관기관, 지역사회 등 모든 이해관계자의 인권 준수를 위해 노력한다.

다섯째, 안전의식을 가지고 위험예방에 최선을 다한다.

여섯째, 지역사회의 일원으로서 사회공헌활동 등 지역사회 발전에 적극 참여한다.

다시 한 번 깨끗하고 공정하고 일 잘하는
KOTRA가 될 것임을 약속드리며,
여러분의 따뜻한 격려와 적극적인 협조를 당부드립니다.

kotra
대한무역투자진흥공사

클린신고센터(부패신고채널)
전화: 02-3460-7010 Email: clean@kotra.or.kr Fax: 02-3460-7902
우편: 서울시 서초구 헌릉로 13 감사실 행동강령책임관

우리기업이 꼭 알아야 할 중국개인정보보호법 가이드북

KOTRA자료 22-086

발 행 일	2022년 7월
발 행 인	유정열
발 행 처	대한무역투자진흥공사(KOTRA)
주 소	서울시 서초구 헌릉로13
전 화	1600-7119
홈 페 이 지	www.kotra.or.kr
문 의 처	베이징무역관(86-10-6410-6162)

• ISBN: 979-11-402-0354-3 (95320)