EQST insight

개인정보보호법 개정, 전문 컨설팅을 활용한 ISMS-P 대응 전략

전략컨설팅담당 김영우 책임

■ 개요

23년 9월 15일부터 개정된 개인정보보호법이 시행됐다. 이 개정은 2020년 데이터 3법 개정 이후, 정보 주체의 권리보호를 강화하고 글로벌 규범과의 상호운용성을 확보하려는 목적으로 전면 개정이 이뤄졌다. 이로 인해 기업에서 유지하고 있는 정보보호 및 개인정보보호 관리 체계 인증(이하 ISMS-P)에도 일부 개정내용이 적용됐다. 개정내용은 개인정보보호위원회 홈페이지를 통해 고시되어 있다.

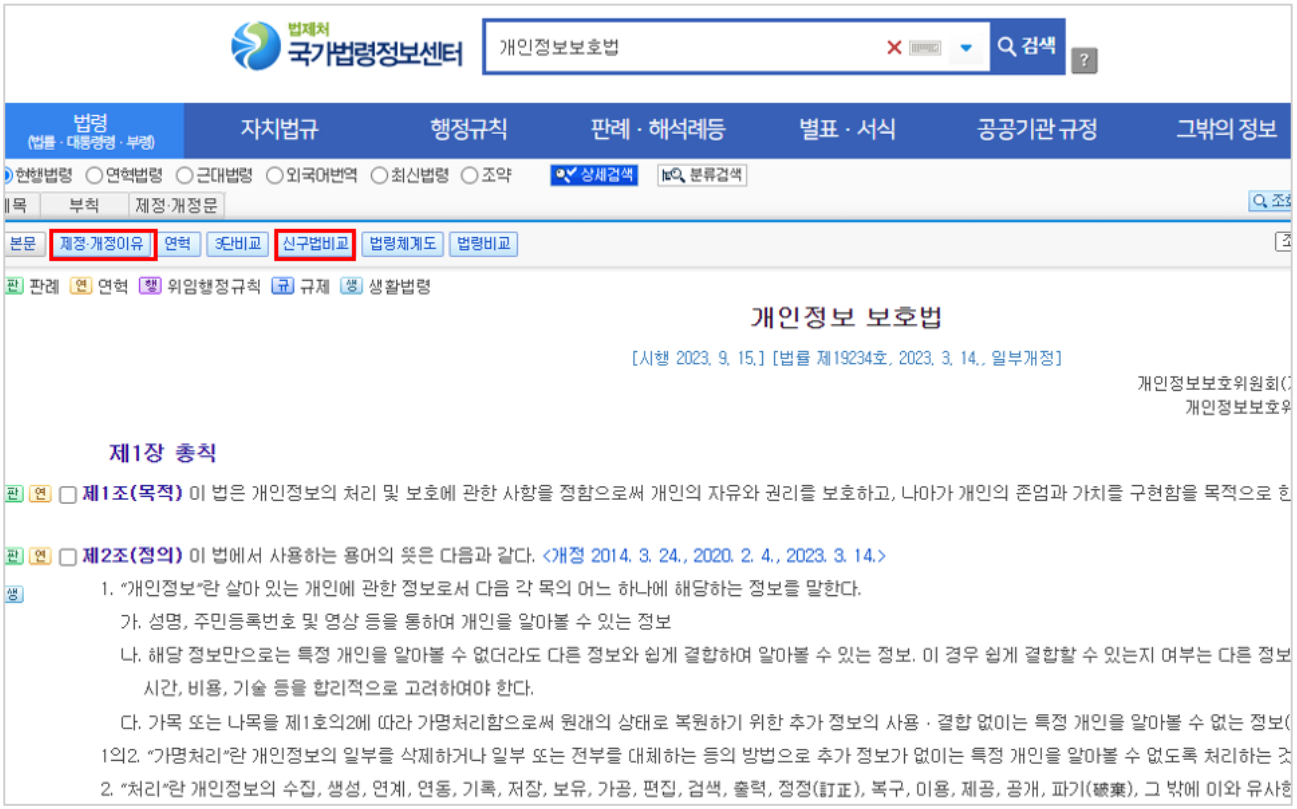
이번 헤드라인에서는 개인정보보호법 개정에 따라 ISMS-P 를 현재 유지 중이거나 신규로 인증 받고자 하는 기업들에게 도움을 제공하기 위해, '23 년도 개정에 따라 변경되는 사항을 분석하여 대응방안을 제시하고자 한다.

■ 개정 법령 및 상세 내용 확인 방법

개정된 개인정보보호법을 확인하는 방법은 다음과 같다. 국가법령정보센터와 개인정보보호위원회 홈페이지를 통해 개정사항을 확인할 수 있으며, 구체적인 개정 내역과 개정사유 등도 열람 가능하다.

1. 개인정보보호법 개정사유 및 개정 항목 확인

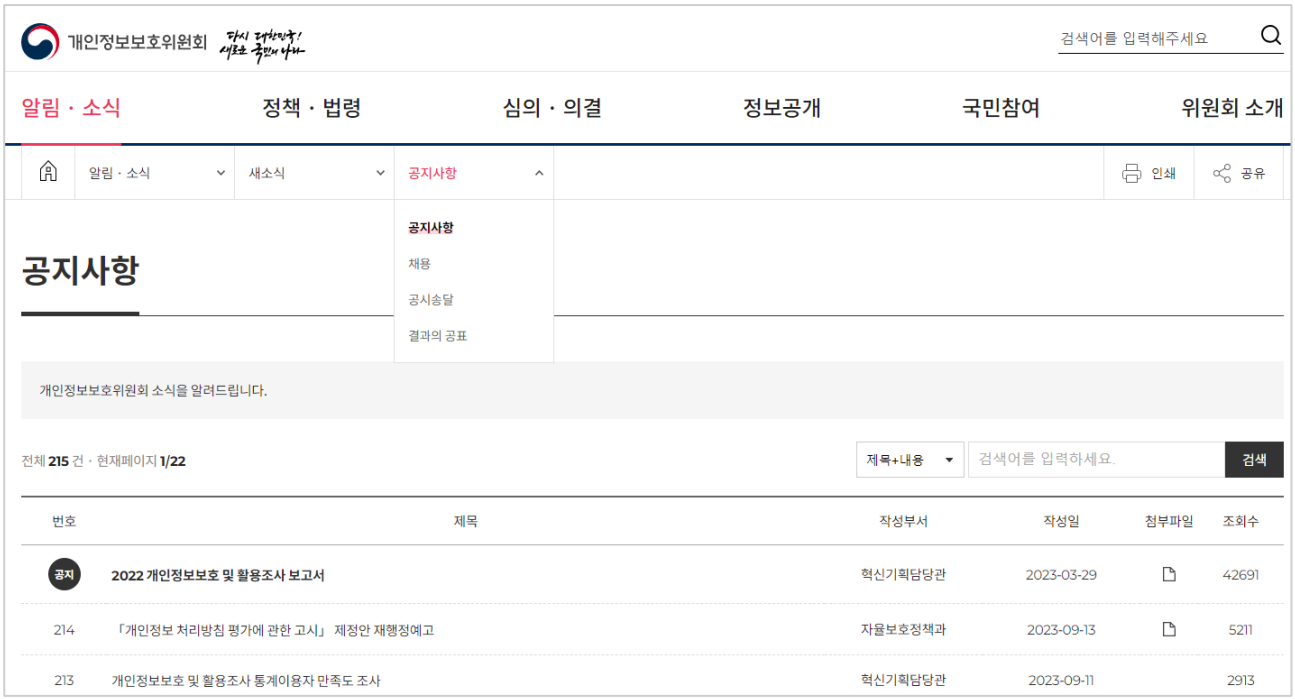
국가법령정보센터 홈페이지 검색창에 “개인정보보호법”이라고 검색어를 입력하면 아래와 같이 해당 법률의 명확한 목적을 확인할 수 있다. 또한, 상단에 제정·개정이유 또는 신구법비교 탭을 클릭하면 해당 내용만 추가로 확인 가능하다.



출처: 국가법령정보센터(www.law.go.kr)

2. 입법 및 행정 예고 확인

개인정보보호위원회 홈페이지 접속 후 알림·소식 탭 내 공지사항을 클릭하면 개인정보보호법 개정과 관련된 내용을 확인할 수 있다.



출처: 개인정보보호위원회(www.pipc.go.kr)

■ ISMS-P 인증 통제항목 매핑

개인정보보호법 개정에 따른 ISMS-P 인증 통제항목을 매핑했다. 그 결과, 주요 개정사항 중 이동형 영상기기규정과 정보통신서비스 특례규정 외 4 개(개인정보보호법상의 원칙은 법적변경사항이 아니므로 제외) 영역에 총 21 개 항목의 ISMS-P 인증 통제항목이 매핑 됐다. 이에 대한 내용은 다음과 같다.

〈표 1〉 개인정보보호 대비 ISMS-P 인증 통제항목

개정 개인정보보호법	ISMS-P 인증 통제항목(21 개 항목)	
이동형 영상기기규정	3.1.6	영상정보처리기기 설치운영
정보통신서비스 특례규정 정비 (온·오프라인 규제 일원화)	1.1.5	정책 수립
	2.5.4	비밀번호 관리
	2.10.8	패치관리
	3.2.1	개인정보 현황관리
	3.4.1	개인정보 파기
동의 받는 방법 및 추가적인 이용·제공	3.1.1	개인정보 수집·이용
	3.1.2	개인정보의 수집동의
	3.1.5	개인정보 간접수집
	3.3.2	개인정보 처리 업무 위탁
	3.5.3	정보주체에 대한 통지
개인정보의 사적 목적 이용 금지	3.2.4	개인정보 목적 외 이용 및 제공
공공시스템운영기관 특례 등 안전성 확보조치	1.1.4	범위 설정
	2.1.2	조직의 유지관리
	2.5.6	접근권한 검토
	2.9.4	로그 및 접속기록 관리
	2.9.5	로그 및 접속기록 점검
국외 이전 및 중지 명령	3.3.4	개인정보 국외이전
개인정보보호법상의 원칙을 중심으로 인증 기준 체계 정비	2.4.7	업무환경 보안
	2.6.3	응용프로그램 접근
	3.2.5	가명정보 처리

출처: 개인정보보호위원회고시 제 2023-8 호, 2023. 10. 5., 및 과학기술정보통신부고시 제 2023-33 호, 2023. 10. 5., 일부개정,

2023 정보보안&개인정보보호 컨퍼런스-참고자료(제목 : 개인정보 보호법 개정 주요내용)

■ 개인정보보호법 주요 개정내용(ISMS-P 매핑 기준)

ISMS-P 통제항목과 연계된 개인정보보호법의 주요 개정내용은 다음과 같다.

① 이동형 영상처리 기기의 운영 기준 마련
② 정보통신서비스 제공자 등에 대한 특례 규정을 일반 규정으로 정비하여 정보통신서비스 제공자와 오프라인 개인정보처리자에 대한 규제를 일원화
③ 개인정보 수집·이용의 법적 근거를 일부 완화
④ 개인정보 이용에 대한 기준 강화
⑤ 주요 공공시스템을 운영하는 기관 등에 대한 안전조치 기준 강화
⑥ 개인정보 국외 이전 요건을 확대하여 국제기준에 부합

〈표 2〉 ISMS-P 통제항목과 연계된 개인정보보호법 주요 개정 내용

개정된 개인정보보호법	개정안 핵심 내용
이동형 영상기기규정	(개정내용)**공개된 장소** 등에서 **업무 목적**으로 이동형 영상정보처리기기를 이용하여 개인영상정보를 촬영하는 행위를 **원칙적으로 제한**
	(예외)개인정보 수집·이용 사유에 해당하거나, 정보주체가 촬영 사실을 알 수 있었음에도 **거부의사를 밝히지 않는 경우 예외적 허용**
	촬영을 하는 경우에는 **불빛, 소리, 안내판, 서면, 안내방송** 등으로 **촬영 사실을 표시**
	(시행령)**이동형 영상기기의 구체적인 범위**, 목욕실·화장실 등에서 영상기기 **운영 제한의 예외 사유, 촬영 사실 표시에 대한 방법** 등 규정 신설
정보통신서비스 특례규정 정비 (온·오프라인 규제 일원화)	(개정내용)정보통신서비스 특례 규정을 일반 규정과 일원화하여 모든 개인정보처리자 대상 **'동일행위-동일규제' 원칙 적용**
	일반 규정과 **유사·중복되는 특례 규정**은 **일반 규정으로 통합·정비**하여 온-오프라인 사업자 간 상이한 규정 단일화
	특례 규정에만 있는 손해배상 보장 제도, 국내 대리인 지정제도, 개인정보 이용 내역 통지 등은 **일반규정으로 전환하여 확대 적용**
동의 받는 방법 및 추가적인 이용·제공	정보주체의 **실질적 동의권을 보장**하고, 기업 등의 **합리적인 개인정보 수집·활용**을 지원하기 위한 동의제도 개선
	정보통신서비스 특례의 **'필수동의' 규정을 정비**하여 '동의 만능주의' 현상을 개선, **동의 이외의** 개인정보 **적법 처리요건 활성화**
	코로나 19 등 **공중위생 목적인 경우도 수집·이용 요건**에 추가
	국민 생명 등 보호를 위해 **급박한 경우 유연하게 대응**할 수 있도록 처리 요건을 개선
	(시행령)**유효한 동의 기준**을 명확히 하고, **동의 없이 처리**할 수 있는 개인정보에 대하여는 **법적 근거를 구분**하여 **처리방침에 공개**하도록 하여 필수동의 관행을 개선
개인정보의 사적 목적 이용 금지	(개정내용)**제 57 조 제 3 호 금지행위** 규정에 정당한 권한 없이 허용된 권한을 초과하여 **타인의 개인정보를 '이용'하는 행위**를 추가
공공시스템운영기관 특례 등 안전성 확보조치	(시행령)국민의 개인정보를 **대규모로 처리하고 있는 공공기관**에 대하여 **공공시스템 안전조치 강화, 개인정보파일 등록 정비**, 개인정보 **영향평가 결과 공개** 등을 통해 안전성과 투명성 강화
	주요 공공시스템을 운영하는 기관 등에 대한 안전조치 기준강화
	공공기관의 개인정보파일 등록 대상 정비
	공공기관의 개인정보 영향평가 결과 공개 근거 마련
국외 이전 및 중지 명령	(개정내용)해외 법제와 상호 운용성 강화를 위해 동의 이외의 **국외이전 적법 요건을 다양화**하고, **중지명령권을 신설**하여 보호조치 강화
	국외이전 요건을 **개인정보보호 인증**을 받은 경우, **이전되는 국가 또는 국제기구의 개인정보 보호 수준이 보장된다고 인정하는 경우** 등으로 다양화
	법 위반 또는 개인정보가 이전되는 국가 등이 개인정보를 적정하게 보호하고 있지 않아 **정보주체에게 피해가 발생할 우려가 현저한 경우** 등에 해당할 때 **개인정보처리자에 대한 국외이전 중지 명령권** 신설

출처: 2023 정보보안&개인정보보호 컨퍼런스-참고자료(제목 : 개인정보 보호법 개정 주요내용)

■ ISMS-P 고시 개정 내용

법률 개정에 따라 “개인정보보호위원회고시 제 2023-08 호-「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」”가 2023.10.5 일부개정으로 시행됐다. 해당 ISMS-P 통제항목을 분석한 결과, 아래 표와 같이 5 가지로 분류된다.

〈표 3〉 ISMS-P 개정된 통제항목의 분류 기준

번호	내용	변경 건
①	3.2.3 항목 세부점검항목 일부 이관	3 건
②	항목명 변경	11 건
③	시행령 개정사항을 반영하여 인증기준 정비	7 건
④	신설	1 건
⑤	삭제	2 건

출처: 개인정보보호위원회고시 제2023-8 호, 2023. 10. 5., 및 과학기술정보통신부고시 제2023-33 호, 2023. 10. 5., 일부개정

〈표 3〉 ISMS-P 개정된 통제항목의 분류 기준을 통해 분석한 상세 내용은 다음과 같다.

〈표 4〉 ISMS-P 고시 개정에 따른 상세 변경내역

ISMS-P 통제항목				변경내역
기존		변경		
2.4.7	업무환경 보안	2.4.7	업무환경 보안	① 3.2.3 항목 세부점검항목 일부 이관
2.6.3	응용프로그램 접근	2.6.3	응용프로그램 접근	① 3.2.3 항목 세부점검항목 일부 이관
2.12.1	재해·재난 대비 안전조치	2.12.1	재해·재난 대비 안전조치	② 항목명 변경
3.1.2	개인정보 수집 동의	3.1.1	개인정보 수집·이용	② 항목명 변경 ③ 시행령 개정사항을 반영하여 인증기준 정비
3.1.1	개인정보 수집 제한	3.1.2	개인정보 수집 제한	③ 시행령 개정사항을 반영하여 인증기준 정비
3.1.5	간접수집 보호조치	3.1.5	개인정보 간접수집	② 항목명 변경 ③ 시행령 개정사항을 반영하여 인증기준 정비
3.1.6	영상정보처리기기 설치운영	3.1.6	영상정보처리기기 설치·운영	③ 시행령 개정사항을 반영하여 인증기준 정비
3.1.7	홍보 및 마케팅 목적 활용 시 조치	3.1.7	마케팅목적의 개인정보 수집·이용	② 항목명 변경
3.2.3	개인정보 표시제한 및 이용 시 보호조치	-	-	⑤ 삭제
3.2.4	이용자 단말기 접근 보호	3.2.3	이용자 단말기 접근보호	② 항목명 변경
-	-	3.2.5	가명정보 처리	① 3.2.3 항목 세부점검항목 일부 이관 ③ 시행령 개정사항을 반영하여 인증기준 정비 ④ 신설
3.3.2	업무 위탁에 따른 정보주체 고지	3.3.2	개인정보 처리 업무 위탁	② 항목명 변경 ③ 시행령 개정사항을 반영하여 인증기준 정비
3.3.3	영업의 양수 등에 따른 개인정보의 이전	3.3.3	영업의 양수 등에 따른 개인정보 이전	② 항목명 변경
3.3.4	개인정보의 국외이전	3.3.4	개인정보 국외이전	② 항목명 변경
3.4.1	개인정보의 파기	3.4.1	개인정보 파기	② 항목명 변경
3.4.3	휴면 이용자 관리	-	-	⑤ 삭제
3.5.1	개인정보처리방침 공개	3.5.1	개인정보 처리방침 공개	② 항목명 변경
3.5.3	이용내역 통지	3.5.3	정보주체에 대한 통지	② 항목명 변경 ③ 시행령 개정사항을 반영하여 인증기준 정비

출처: 개인정보보호위원회고시 제2023-8호, 2023. 10. 5., 및 과학기술정보통신부고시 제2023-33호, 2023. 10. 5., 일부개정

,

■ ISMS-P 통제항목에 대한 준비 사항

고시된 ISMS-P 인증기준 통제항목에 따라 준비해야 할 사항을 살펴본다. 먼저, **개인정보처리방침 개정 및 개인정보관련 지침 수립이 필요**하다. 그리고, 기존 통제항목에서 변경된 내용을 확인하여 기업 별 시스템 환경에 맞춘 준비를 해야 한다. 앞서 제시한 〈표 4〉에서 5 가지 변경내역 기준 중 ② 항목명 변경, ⑤ 삭제 항목을 제외하고 3 가지 기준(이관, 정비, 신설)에 대한 통제항목 별 상세 내용과 준비사항은 다음과 같다.

〈표 5〉 ISMS-P 개정항목에 대한 준비 사항

통제항목		상세 내용	ISMS-P 인증심사 준비사항(증적)
2.4.7	업무환경 보안	공용 사무용 기기 및 개인 업무환경을 통해 개인정보 및 중요정보가 비인가자에게 노출 또는 유출되지 않도록 보호대책을 수립・이행	1) 출력·복사물 보호조치 현황
2.6.3	응용프로그램 접근	사용자별 업무 및 접근 정보의 중요도 등에 따라 응용프로그램 접근권한을 제한하고, 불필요한 정보 노출을 최소화할 수 있도록 기준을 수립 적용	1) 개인정보 마스킹 적용 화면
3.1.1	개인정보 수집·**이용**	**개인정보는 적법하고 정당하게 수집·이용하여야 하며, 정보주체의 동의를 근거로 수집 시 적법한 방법으로 정보주체의 동의를 받아야 함.** 만 14 세 미만 아동의 개인정보를 수집 시 법정대리인의 동의를 받아야 **하며 법정대리인이 동의하였는지 확인**	1) 법적 기준에 따라 이용·제공 내역에 통지 관련 지침 수립 2) 이용·제공 내역에 통지 결과 3) 개인정보처리방침
3.1.2	개인정보 수집 제한	**개인정보를 수집하는 경우 처리 목적에 필요한 최소한의 개인정보만을** 수집. **정보주체가 선택적으로 동의할 수 있는 사항 등에 동의하지 아니한다는** 이유로 **정보주체에게 재화 또는** 서비스의 제공을 거부하지 않아야 함	1) 개인정보처리방침
3.1.5	**개인정보 간접수집**	정보주체 이외로부터 개인정보를 수집하거나 **제 3 자로부터** 제공받는 경우, 업무에 필요한 최소한의 개인정보를 **수집하거나 제공받아야 함.** 법령에 근거하거나 정보주체의 요구가 있으면 수집 출처, 처리목적, 처리정지의 요구권리를 알려야 함	1) 개인정보처리방침
3.1.6	영상정보처리기기 설치·운영	**고정형 영상정보처리기기를 공개된 장소에 설치·운영하거나 이동형 영상정보처리기기를 공개된 장소에서 업무를 목적으로** 운영하는 경우 설치 목적 및 위치에 따라 법적 요구사항을 준수하고 적절한 보호대책을 수립·이행	1) 영상정보처리기기 관련 지침 개정 2) 개인정보처리방침
3.2.5	가명정보 처리	가명정보를 처리 시 목적제한, 결합제한, 안전조치, 금지의무 등 법적 요건을 준수하고 적정 수준의 가명처리를 보장할 수 있도록 가명처리 절차를 수립·이행	1) 가명정보 처리 절차 및 결과 2) 가명 처리 결과 (가명정보 사용 시) 3) 개인정보처리방침 (가명정보 이용·제공에 관한 사항)

통제항목		상세 내용	ISMS-P 인증심사 준비사항(증적)
3.3.2	**개인정보 처리 업무 위탁**	개인정보 처리업무를 제 3 자에게 위탁하는 경우 위탁하는 업무의 내용과 수탁자 등 관련사항을 **공개하고 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁 시 위탁하는 업무의 내용과 수탁자를** 정보주체에게 알려야 함	1) 제 3 자 위탁관련 규정 및 지침 개정 2) 개인정보처리방침
3.5.3	**정보주체에 대한 통지**	개인정보의 이용·**제공** 내역 등 정보주체에게 통지하여야 할 사항을 파악하여 그 내용을 주기적으로 통지	1) 법적 기준에 따라 이용·제공 내역에 통지 관련 지침 수립 2) 이용·제공 내역에 통지 결과 3) 개인정보처리방침

*ISMS-P 변경된 고시 관련하여 세부지침이 나오지 않아 일부 추가 및 변경될 수 있음

출처: 개인정보보호위원회고시 제2023-8호, 2023. 10. 5., 및 과학기술정보통신부고시 제2023-33호, 2023. 10. 5., 일부개정

■ 맺음말

이번 개인정보보호법 개정에 따라 ISMS-P 인증심사를 유지하거나 신규도입을 준비하는 기업들은 앞서 소개한 개정사항을 확인 후 대비해야 한다. 특히, 주요 개정사항인 개인정보 수집·이용, 개인정보 수집 제한, 개인정보 간접수집, 영상정보처리기기 설치·운영, 가명정보 처리, 개인정보 처리 업무 위탁, 정보주체에 대한 통지 항목 등에 대한 준비가 필요하다.

구체적으로, 기업들은 개정 이후 ISMS-P 인증심사를 준비하기 위해 **개인정보 처리방침 개정**을 비롯해 개인정보 수집·이용, 영상정보처리기기 설치·운영, 개인정보 처리 업무 위탁, 정보주체에 대한 통지에 대해 **개인정보관련 지침 수립이 필요하다.** 공공기관의 경우에는 강화된 '개인정보의 안전성 확보조치 기준 고시' 내용에 따라 추가 **결함들이 도출될 수 있어 추가적인 점검이 필요**하다.

SK 쉴더스는 최고 수준의 전문인력을 기반으로 ISMS-P 인증심사 시 필요한 개인정보 관련 처리방침 개정과 지침 수립, 도출될 수 있는 결함 점검 등을 지원하고 있다. 또한, 개인정보보호 컨설팅을 비롯해 컴플라이언스 컨설팅, 정보보호 관리체계 컨설팅, 모의해킹 컨설팅, 개발 보안 컨설팅, 종합 정보보호 컨설팅 등 기업 별 환경을 고려한 다양한 맞춤형 컨설팅 서비스를 제공하고 있다.

이러한 **SK 쉴더스 컨설팅**을 통해 지속적으로 변화하는 컴플라이언스에 효과적이고 체계적으로 대응하길 바란다. 보다 자세한 내용은 SK 쉴더스 공식 블로그를 통해 확인할 수 있다.

■ 참고문헌

1. 국가법령정보센터, https://www.law.go.kr/

- 개인정보 보호법 [시행 2023. 9. 15.] [법률 제 19234 호, 2023. 3. 14., 일부개정]

- 개인정보 보호법 시행령 [시행 2023. 9. 15.] [대통령령 제 33723 호, 2023. 9. 12., 일부개정]

2. 개인정보보호위원회, https://www.pipc.go.kr/np/

- 개인정보의 안전성 확보조치 기준 [시행 2023. 9. 22.] [개인정보보호위원회고시 제 2023-6 호, 2023. 9. 22., 일부개정]

- 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 [개인정보보호위원회고시 제 2023-8 호, 2023. 10. 5., 일부개정], [과학기술정보통신부고시 제 2023-33 호, 2023. 10. 5., 일부개정]

3. KISA, 정보보호 및 개인정보관리체계 https://isms.kisa.or.kr/main/

4. 2023 정보보안&개인정보보호 컨퍼런스-참고자료(제목 : 개인정보 보호법 개정 주요내용)