개인정보 처리방침

에스제이엘파트너스 유한책임회사(이하 "회사")는「개인정보 보호법」제 30 조에 따라 정보주체의 개인정보를 보호하고 이와 관련한 고충을 신속하고 원활하게 처리할 수 있도록 다음과 같이 개인정보 처리방침을 수립·공개합니다.

본 처리방침은 2026 년 10 월 23 일부터 적용됩니다.

제 1 조 (개인정보의 처리 목적, 처리 항목 및 보유 기간)

회사는 다음의 목적을 위하여 필요한 최소한의 개인정보를 처리하며, 처리 목적이 변경되는 경우에는「개인정보 보호법」제 18 조에 따라 별도의 동의를 받는 등 필요한 조치를 이행합니다. 회사는 법령에 따른 보유·이용 기간 또는 정보주체로부터 수집 시 동의받은 기간 내에서 개인정보를 처리·보유합니다.

구분	처리 목적	처리 항목	처리 근거	보유 기간
대외 문의(이메일·전화)	문의 접수 및 회신	성명, 이메일 주소, 연락처, 소속, 문의 내용	정보주체가 문의를 위하여 제공한 정보의 처리(제 15 조제 1 항제 6 호)	문의 처리 완료 후 1 년
투자자(LP) 관련	출자약정 체결·이행, 투자자 보고, 고객확인(KYC) 및 자금세탁방지	법인 투자자의 대표자·실제소유자·업무담당자의 성명, 생년월일, 국적, 직위, 연락처, 이메일 주소, 신분증 사본 등	계약 체결·이행(제 15 조제 1 항제 4 호), 법령상 의무 준수(제 15 조제 1 항제 2 호,「특정 금융거래정보의 보고 및 이용 등에 관한 법률」)	관련 펀드의 청산 완료일부터 10 년(분쟁 대응 및 관계 법령에 따른 자료 요구 대응). 다만 고객확인 자료는 특정금융정보법 제 5 조의 4 에 따라 거래관계 종료일부터 최소 5 년
거래 상대방 및 투자대상회사 관련	투자 검토·실사, 계약 체결·이행, 사후 관리	임직원·담당자의 성명, 소속, 직위, 연락처, 이메일 주소	계약 체결·이행(제 15 조제 1 항제 4 호), 회사의 정당한 이익(제 15 조제 1 항제 6 호)	관련 펀드의 청산 완료일부터 10 년(투자가 이루어지지

구분	처리 목적	처리 항목	처리 근거	보유 기간
				않은 검토 건은 검토 종료일부터 10 년)
임직원 및 채용 지원자	채용, 인사·급여 관리 및 법령상 의무 이행	별도의 「임직원 개인정보 처리 안내 및 동의서」에 따름	같은 안내서 및 동의서에 따름	같은 안내서 및 동의서에 따름

다만, 관계 법령 위반에 따른 수사·조사 등이 진행 중인 경우에는 해당 수사·조사 종료 시까지 보유합니다.

제 2 조 (개인정보의 제 3 자 제공)

1. 회사는 정보주체의 개인정보를 제 1 조의 처리 목적 범위에서만 처리하며, 정보주체의 동의, 법률의 특별한 규정 등「개인정보 보호법」제 17 조 및 제 18 조에 해당하는 경우에만 개인정보를 제 3 자에게 제공합니다.
2. 회사는 법령에 따른 신고·등기·보고 등을 위하여 금융감독원, 법원(등기소), 국세청 등 관계 기관에 개인정보를 제공하거나, 감독기관 및 수사기관이 법령에 따라 요청하는 경우 해당 법령에서 정한 범위에서 개인정보를 제공할 수 있습니다.
3. 회사는 펀드 운용과 관련하여 다음과 같이 개인정보를 제공합니다.

제공받는 자	제공 목적	제공 항목	보유 기간
펀드 수탁은행 펀드 사무수탁사 및 회계법인	펀드 자금 집행 및 수탁 업무 펀드 회계 및 세무처리 등기업무	법인 투자자의 대표자·실제소유자·업무 담당자의 성명, 개인 투자자의 성명, 생년월일, 국적, 직위, 연락처, 이메일 주소, 신분증 사본, 인감증명서 또는 본인서명사실확인서 등	제공 목적 달성 시까지

제 3 조 (개인정보 처리업무의 위탁)

1. 회사는 원활한 업무 처리를 위하여 다음과 같이 개인정보 처리업무를 위탁하고 있습니다.

수탁자	위탁 업무
딜로이트안진회계법인	임직원 급여 계산, 원천세 신고, 4 대 보험 처리

수탁자	위탁 업무
고우넷(Gownet)	IT 시스템 유지보수, 계정 관리 및 보안 지원
하나투어	임직원 출장 항공·숙박 예약 및 비자 발급 대행
웰스컴	임직원 명함 제작
SFC	임직원 주차권 발급
사철농원	경조사 화환 발송
플립	홈페이지 제작·운영
에스원	사무실 출입통제 시스템 운영, 방범 및 CCTV 영상정보 관리
Microsoft Corporation	Microsoft 365 클라우드 서비스(이메일, 문서 저장 등) 제공
Anthropic, PBC	AI 기반 업무 지원 서비스(Claude) 제공

2. 회사는 위탁계약 체결 시「개인정보 보호법」제 26 조에 따라 위탁업무 수행 목적 외 처리 금지, 기술적·관리적 보호조치, 재위탁 제한, 수탁자에 대한 관리·감독, 손해배상 등 책임에 관한 사항을 계약서 등 문서에 명시하고, 수탁자가 개인정보를 안전하게 처리하는지 감독합니다.
3. 위탁업무의 내용이나 수탁자가 변경될 경우에는 지체 없이 본 개인정보 처리방침을 통하여 공개합니다.

제 4 조 (개인정보의 국외 이전)

회사는 다음과 같이 개인정보를 국외로 이전하고 있습니다. 클라우드 및 AI 업무 지원 서비스(Microsoft, Anthropic)는 처리위탁·보관에 따른 이전으로「개인정보 보호법」 제 28 조의 8 제 1 항제 3 호에 따라 공개하며, 정보 서비스 계정 개설(S&P Global)은 임직원의 별도 동의(같은 항 제 1 호)를 받아 제공합니다.

이전받는 자 (연락처)	이전 국가	이전 일시 및 방법	이전 항목	이전 목적	보유 기간
Microsoft Corporation (privacy@microsoft.com / +1 425-882- 8080	대한민국(저장), 미국 및 Microsoft 재수탁자 소재국(운영·기술지원 목적 접근)	서비스 이용 시 네트워크를 통한 전송	임직원 및 업무 상대방의 성명, 이메일 주소, 업무 자료에 포함된 개인정보	이메일 및 문서 저장 등 클라우드 서비스 이용	계정 삭제 또는 계약 종료 시까지

이전받는 자 (연락처)	이전 국가	이전 일시 및 방법	이전 항목	이전 목적	보유 기간
Anthropic, PBC (privacy@anthropic.com)	미국	서비스 이용 시 네트워크를 통한 전송	임직원의 성명, 이메일 주소, 입력된 업무 자료에 포함된 개인정보	AI 기반 업무 지원 서비스 이용	대화 삭제 또는 계약 종료 시까지(삭제 후 30 일 이내 파기). 단, 이용정책 위반 탐지 시 최대 2 년
S&P Global Inc. (privacy@spglobal.com, +1 855-529-1761)	미국	정보 서비스 계정 개설 시 및 이용 시 네트워크를 통한 전송	임직원의 성명, 직위, 연락처, 이메일 주소	정보 서비스 이용계정 개설 및 이용(임직원의 별도 동의에 따른 국외 제공)	서비스 이용계약 종료 시까지

정보주체는 회사의 개인정보보호책임자에게 연락하여 개인정보의 국외 이전을 거부할 수 있습니다. 다만, 이전을 거부하면 해당 서비스를 통한 업무 처리가 제한될 수 있습니다.

제 5 조 (개인정보의 파기 절차 및 방법)

1. 회사는 개인정보 보유 기간이 경과하거나 처리 목적이 달성되는 등 개인정보가 불필요하게 되었을 때에는 지체 없이 해당 개인정보를 파기합니다.
2. 정보주체로부터 동의받은 보유 기간이 경과하거나 처리 목적이 달성되었음에도 다른 법령에 따라 개인정보를 계속 보존하여야 하는 경우에는, 해당 개인정보를 별도의 데이터베이스(DB)로 옮기거나 보관 장소를 달리하여 보존합니다.
3. 파기 방법: 전자적 파일 형태의 정보는 복구·재생할 수 없는 기술적 방법으로 삭제하고, 종이 문서는 분쇄하거나 소각합니다.

제 6 조 (정보주체와 법정대리인의 권리·의무 및 행사 방법)

1. 정보주체는 회사에 대하여 언제든지 개인정보 열람, 정정·삭제, 처리정지 및 동의 철회 등을 요구할 수 있습니다.

2. 권리 행사는 서면, 전자우편 등을 통하여 할 수 있으며, 회사는 이에 대해 지체 없이 조치합니다. 정보주체의 법정대리인이나 위임을 받은 자 등 대리인을 통하여도 권리를 행사할 수 있으며, 이 경우 위임장을 제출하여야 합니다.
3. 개인정보 열람 및 처리정지 요구는「개인정보 보호법」제 35 조제 4 항, 제 37 조제 2 항에 따라 제한될 수 있으며, 다른 법령에서 수집 대상으로 명시된 개인정보는 삭제를 요구할 수 없습니다.
4. 회사는 권리 행사를 한 자가 본인이거나 정당한 대리인인지를 확인합니다.
5. 회사는 만 14 세 미만 아동의 개인정보를 수집하지 않습니다.

제 7 조 (개인정보의 안전성 확보조치)

회사는「개인정보 보호법」제 29 조에 따라 다음과 같이 안전성 확보에 필요한 조치를 하고 있습니다.

- **관리적 조치:** 개인정보보호책임자 지정, 개인정보 내부 관리계획 수립·시행 및 연 1 회 이행 실태 점검, 임직원 정보보안 교육, 근로계약에 따른 비밀유지 의무 부과
- **기술적 조치:** 직무에 따른 최소한의 접근권한 부여(부여·변경 시 COO 확인), 방화벽·VPN·엔드포인트 보안 프로그램 운영, 접속기록 정기 검토, 승인 없는 기밀자료 전송·출력 제한, 출입통제용 생체인식정보(지문) 암호화 저장
- **물리적 조치:** 출입통제 시스템(에스원) 운영 및 CCTV 설치, 서류 보관실 및 문서 캐비닛 잠금장치 적용

제 8 조 (영상정보처리기기의 설치·운영)

회사는 사무실 내부에 다음과 같이 영상정보처리기기(CCTV)를 설치·운영하고 있습니다.

구분	내용
설치 목적 및 근거	시설 안전 및 화재·도난 방지, 임직원 안전 및 회사 자산 보호(「개인정보 보호법」제 15 조제 1 항제 6 호)
설치 대수·위치 및 촬영 범위	9 대 / 사무실 출입구, 복도, 사무공간, 회의실 등 / 해당 구역
촬영 시간	24 시간
보관 기간	촬영일로부터 10 년. 다만 사고·분쟁 조사 등에 필요한 영상은 해당 조사 또는 분쟁이 종료될 때까지 별도 보관
보관 기간 설정 사유	도난·분실, 문서 유출, 직장 내 사고 등은 상당 기간이 지난 후 인지되거나 소송 등 분쟁으로 제기될 수 있으므로,「민법」상 채권의 소멸시효(제 162 조제 1 항, 10 년) 및 불법행위로 인한 손해배상청구권의

구분	내용
	행사기간(제 766 조제 2 항, 불법행위를 한 날부터 10 년) 동안 사실관계 확인 및 분쟁 대응을 위함. 보관 기간이 지난 영상은 지체 없이 파기
관리 책임자 및 접근 권한자	개인정보보호책임자(제 11 조) / 관리 위탁: 에스원
열람 등 요구	정보주체는 개인정보보호책임자에게 본인이 촬영된 영상의 열람·존재확인을 요구할 수 있으며, 회사는 다른 정보주체의 사생활 침해 우려 등 법령에서 정한 사유가 없는 한 지체 없이 조치합니다.

제 9 조 (개인정보 자동 수집 장치의 설치·운영 및 거부)

- 회사 홈페이지에는 개인정보 입력란이 없으며, 회사는 홈페이지에서 쿠키 등 개인정보를 자동으로 수집하는 장치를 설치·운영하지 않습니다.

제 10 조 (자동화된 결정, 가명정보 및 민감정보)

회사는 완전히 자동화된 시스템으로 정보주체에게 중대한 영향을 미치는 결정을 하지 않으며, 가명정보를 처리하지 않습니다. 회사가 제공하는 서비스를 통하여 정보주체의 민감정보가 공개될 가능성은 없습니다.

회사는 임직원의 출입통제를 위한 생체인식정보(지문)를 별도 동의를 받아 처리하며, 감독당국 제출 보고서에 임원으로 기재되는 자(기재 예정자 포함)에 한하여 그 범죄경력 등 결격사유 관련 정보를 「자본시장과 금융투자업에 관한 법률」 및 「금융회사의 지배구조에 관한 법률」에 따른 임원 결격사유 확인 및 금융감독원 보고를 위하여 법령에 따라 처리합니다.

제 11 조 (개인정보보호책임자)

회사는 개인정보 처리에 관한 업무를 총괄하고 정보주체의 불만 처리 및 피해 구제 등을 위하여 다음과 같이 개인정보보호책임자를 지정하고 있습니다.

구분	내용
개인정보보호책임자	성명: 김규희 / 직책: COO(최고운영책임자)
연락처	전화: 02-6911-9701 / 이메일: public@sjlpartners.com

제 12 조 (권익침해 구제 방법)

정보주체는 개인정보 침해로 인한 구제를 받기 위하여 다음 기관에 분쟁 해결이나 상담 등을 신청할 수 있습니다.

- 개인정보분쟁조정위원회: (국번 없이) 1833-6972 (www.kopico.go.kr)

- 개인정보침해신고센터: (국번 없이) 118 (privacy.kisa.or.kr)
- 대검찰청: (국번 없이) 1301 (www.spo.go.kr)
- 경찰청: (국번 없이) 182 (ecrm.police.go.kr)

제 13 조 (개인정보 처리방침의 변경)

본 개인정보 처리방침은 2026 년 10 월 23 일부터 적용되며, 내용이 변경되는 경우 시행 7 일 전부터 홈페이지를 통하여 공지합니다. 이전 처리방침은 홈페이지에서 확인할 수 있습니다.

- 이전 개인정보 처리방침(Privacy Policy): 2019 년 12 월 ~ 2026 년 10 월 23 일 적용

Privacy Policy

SJL Partners, LLC (the "Company") establishes and discloses this Privacy Policy in accordance with Article 30 of the Personal Information Protection Act of Korea ("PIPA") in order to protect the personal information of data subjects and to handle related complaints promptly and smoothly.

This Privacy Policy applies from October 23, 2026.

Article 1 (Purposes of Processing, Items Processed and Retention Periods)

The Company processes only the minimum personal information necessary for the following purposes. If a purpose of processing changes, the Company will take necessary measures, such as obtaining separate consent in accordance with Article 18 of PIPA. The Company processes and retains personal information within the retention period prescribed by law or the period consented to by the data subject at the time of collection.

Category	Purpose	Items	Legal Basis	Retention Period
External inquiries (e-mail and telephone)	Receiving and responding to inquiries	Name, e-mail address, contact number, organization, content of inquiry	Processing of information provided by the data subject for the inquiry (PIPA Art. 15(1)(vi))	1 year after the inquiry is resolved
Investors (LPs)	Execution and performance of capital commitments, investor reporting, customer due diligence (KYC) and anti-money laundering	Name, date of birth, nationality, title, contact number, e-mail address and copy of identification of representatives, beneficial owners and contact persons of corporate investors, etc.	Execution and performance of contracts (PIPA Art. 15(1)(iv)); compliance with legal obligations (PIPA Art. 15(1)(ii); Act on Reporting and Using Specified Financial Transaction Information)	10 years from the completion of liquidation of the relevant fund (for dispute response and responding to requests under applicable laws); provided that customer due diligence records are retained for at least 5 years from the end of the business relationship under Article 5-4 of the Act on Reporting and Using Specified Financial Transaction Information
Counterparties and portfolio companies	Investment review and due diligence, execution and performance of contracts, post-investment management	Name, organization, title, contact number and e-mail address of officers, employees and contact persons	Execution and performance of contracts (PIPA Art. 15(1)(iv)); legitimate interests of the Company (PIPA Art. 15(1)(vi))	10 years from the completion of liquidation of the relevant fund (for reviews not resulting in an investment, 10 years from the end of the review)
Employees and job applicants	Recruitment, HR and payroll management, and	As set out in the separate Employee	As set out in the same Notice & Consent	As set out in the same Notice & Consent

Category	Purpose	Items	Legal Basis	Retention Period
	compliance with legal obligations	Personal Information Notice & Consent		

However, if an investigation or inquiry concerning a violation of applicable laws is in progress, the relevant personal information will be retained until the investigation or inquiry is concluded.

Article 2 (Provision of Personal Information to Third Parties)

1. The Company processes personal information only within the scope of the purposes set out in Article 1 and provides personal information to third parties only where Article 17 or 18 of PIPA applies, such as with the consent of the data subject or under special provisions of law.
2. The Company may provide personal information to relevant authorities, such as the Financial Supervisory Service, the courts (commercial registry offices) and the National Tax Service, for filings, registrations, reports and other purposes required by law, or to supervisory authorities and investigative agencies upon their request under applicable laws, to the extent prescribed by such laws.
3. The Company provides personal information in connection with fund management as follows.

Recipient	Purpose	Items Provided	Retention Period
Fund custodian banks Fund administrators and accounting firms	Fund cash management and custody services Fund accounting and tax processing Registration filings	Names of representatives, beneficial owners and contact persons of corporate investors; names of individual investors; date of birth, nationality, title, contact number, e-mail address, copy of identification, certificate of seal impression or certificate of personal signature, etc.	Until the purpose of provision is achieved

Article 3 (Outsourcing of Personal Information Processing)

1. The Company outsources the processing of personal information as follows for efficient business operations.

Service Provider	Outsourced Services
Deloitte Anjin LLC	Payroll calculation, withholding tax filing and social insurance administration for employees
Gownet	IT system maintenance, account management and security support
Hanatour	Flight and hotel bookings and visa application services for employee business travel
Wellscom	Production of employee business cards
SFC	Issuance of employee parking passes
Sacheol Nongwon	Delivery of flowers for congratulatory and condolence events
Flip	Website development and operation
S-1 Corporation	Operation of office access control system, security services and management of CCTV footage
Microsoft Corporation	Provision of Microsoft 365 cloud services (e-mail, document storage, etc.)

Service Provider	Outsourced Services
Anthropic, PBC	Provision of AI-based work support services (Claude)

2. When entering into an outsourcing agreement, the Company specifies in a contract or other document, in accordance with Article 26 of PIPA, matters including the prohibition of processing for purposes other than the outsourced services, technical and administrative safeguards, restrictions on sub-outsourcing, management and supervision of the service provider, and liability for damages, and supervises whether the service provider processes personal information securely.
3. If the outsourced services or the service providers change, the Company will disclose such changes through this Privacy Policy without delay.

Article 4 (Overseas Transfer of Personal Information)

The Company transfers personal information overseas as follows. Transfers for cloud and AI-based work support services (Microsoft and Anthropic) are made for outsourcing and storage and are disclosed under Article 28-8(1)(iii) of PIPA. Information provided to open accounts for information services (S&P Global) is provided with the separate consent of employees under Article 28-8(1)(i) of PIPA.

Recipient (Contact)	Country	Timing and Method	Items Transferred	Purpose	Retention Period
Microsoft Corporation (privacy@microsoft.com / +1 425-882-8080)	Republic of Korea (storage); United States and countries where Microsoft sub-processors are located (access for operation and technical support)	Transmitted over the network when using the services	Name and e-mail address of employees and business counterparts; personal information contained in work documents	Use of cloud services such as e-mail and document storage	Until account deletion or termination of the agreement
Anthropic, PBC (privacy@anthropic.com)	United States	Transmitted over the network when using the services	Name and e-mail address of employees; personal information contained in work materials entered	Use of AI-based work support services	Until the conversation is deleted or the agreement terminates (destroyed within 30 days after deletion); up to 2 years where a usage policy violation is detected
S&P Global Inc. (privacy@spglobal.com, +1 855-529-1761)	United States	Transmitted over the network when opening and	Name, title, contact number and e-mail address of employees	Opening and use of information service accounts (overseas	Until termination of the service agreement

Recipient (Contact)	Country	Timing and Method	Items Transferred	Purpose	Retention Period
		using an account		provision based on separate employee consent)	

Data subjects may refuse the overseas transfer of their personal information by contacting the Company's Chief Privacy Officer. However, if the transfer is refused, business through the relevant services may be restricted.

Article 5 (Procedures and Methods of Destruction)

1. When personal information becomes unnecessary, such as upon expiry of the retention period or achievement of the purpose of processing, the Company destroys it without delay.
2. Where personal information must continue to be preserved under other laws despite expiry of the retention period consented to by the data subject or achievement of the purpose of processing, the Company transfers it to a separate database or keeps it in a separate storage location.
3. Methods of destruction: electronic files are deleted using technical methods that prevent recovery or reproduction, and paper documents are shredded or incinerated.

Article 6 (Rights and Obligations of Data Subjects and Legal Representatives and How to Exercise Them)

1. Data subjects may at any time request the Company to provide access to, correct or delete their personal information, suspend its processing, or withdraw consent.
2. Such rights may be exercised in writing, by e-mail or by other means, and the Company will take action without delay. Rights may also be exercised through a representative, such as a legal representative or a person authorized by the data subject, in which case a power of attorney must be submitted.
3. Requests for access and suspension of processing may be restricted under Article 35(4) and Article 37(2) of PIPA, and deletion may not be requested for personal information that other laws specify as subject to collection.
4. The Company verifies whether the person exercising the rights is the data subject or a duly authorized representative.
5. The Company does not collect personal information of children under the age of 14.

Article 7 (Measures to Ensure the Security of Personal Information)

The Company takes the following measures necessary to ensure security in accordance with Article 29 of PIPA.

- **Administrative measures:** Designation of a Chief Privacy Officer; establishment and implementation of an internal management plan for personal information protection with an annual review of its implementation; information security training for employees; confidentiality obligations under employment contracts.
- **Technical measures:** Granting of minimum access rights based on job duties (with confirmation by the COO for any grant or change); operation of firewall, VPN and endpoint security programs; regular review of access logs; restrictions on unauthorized transmission or printing of confidential materials; encrypted storage of biometric information (fingerprints) used for access control.
- **Physical measures:** Operation of an access control system (S-1 Corporation) and CCTV; locking devices on the document storage room and document cabinets.

Article 8 (Installation and Operation of Video Surveillance Devices)

The Company installs and operates video surveillance devices (CCTV) within its office as follows.

Item	Details
Purpose and legal basis	Facility safety, prevention of fire and theft, safety of employees and protection of Company assets (PIPA Art. 15(1)(vi))
Number, locations and areas recorded	9 cameras / office entrance, hallways, office work areas, meeting rooms, etc. / the relevant areas
Recording hours	24 hours
Retention period	10 years from the date of recording; provided that footage required for the investigation of incidents or disputes is retained separately until the relevant investigation or dispute is concluded
Reason for retention period	Theft, loss, leakage of documents and workplace incidents may only be discovered, or be raised as litigation or other disputes, a considerable time after they occur. Footage is therefore retained to verify facts and respond to disputes during the extinctive prescription period for claims (Civil Act Art. 162(1), 10 years) and the period for exercising claims for damages arising from tort (Civil Act Art. 766(2), 10 years from the date of the tortious act). Footage is destroyed without delay after the retention period expires.
Manager and persons with access	Chief Privacy Officer (Article 11) / management outsourced to S-1 Corporation
Requests for access	Data subjects may request the Chief Privacy Officer to view, or confirm the existence of, footage in which they appear, and the Company will act without delay unless there are grounds prescribed by law, such as a risk of infringing the privacy of other data subjects.

Article 9 (Installation, Operation and Refusal of Automatic Collection Devices)

The Company's website has no fields for entering personal information, and the Company does not install or operate cookies or other devices that automatically collect personal information on its website.

Article 10 (Automated Decisions, Pseudonymized Information and Sensitive Information)

The Company does not make decisions that significantly affect data subjects using fully automated systems and does not process pseudonymized information. There is no possibility that sensitive information of data subjects will be disclosed through the services provided by the Company.

The Company processes biometric information (fingerprints) of employees for access control with their separate consent. For persons listed as officers in reports submitted to supervisory authorities (including persons expected to be so listed) only, the Company processes information on criminal records and other grounds for disqualification in accordance with applicable laws, in order to confirm whether any ground for disqualification of officers exists under the Financial Investment Services and Capital Markets Act and the Act on Corporate Governance of Financial Companies and to report to the Financial Supervisory Service.

Article 11 (Chief Privacy Officer)

The Company has designated the following Chief Privacy Officer to oversee the processing of personal information and to handle complaints and remedies for data subjects.

Item	Details
Chief Privacy Officer	Name: Anna Kyuhee Kim / Title: Chief Operating Officer (COO)
Contact	Tel: +82-2-6911-9701 / E-mail: public@sjlpartners.com

Article 12 (Remedies for Infringement of Rights)

Data subjects may apply to the following organizations for dispute resolution or consultation regarding infringement of personal information.

- Personal Information Dispute Mediation Committee: 1833-6972 (www.kopico.go.kr)
- Personal Information Infringement Report Center (KISA): 118 (privacy.kisa.or.kr)
- Supreme Prosecutors' Office: 1301 (www.spo.go.kr)
- Korean National Police Agency: 182 (ecrm.police.go.kr)

Article 13 (Changes to this Privacy Policy)

This Privacy Policy applies from October 23, 2026. Any changes will be announced on the Company's website at least 7 days before they take effect. Previous versions of the Privacy Policy are available on the Company's website.

- Previous Privacy Policy: applied from December 2019 to October 23, 2026

This Privacy Policy is prepared in Korean and English. In case of any discrepancy between the two versions, the Korean version shall prevail.