POLÍTICA DE CONFIDENCIALIDAD

POLÍTICA DE CONFIDENCIALIDAD

POLÍTICA DE CONFIDENCIALIDAD, SECRETO PROFESIONAL, RESERVA PERICIAL Y SEGURIDAD CRIPTOGRÁFICA
UNIVERSITÉ EUROPÉENNE DE PARIS - UNIVERSITÉ EUROPÉENNE (SAEJEE — UNIVERSIDAD EUROPEA DE PARÍS)
Referencia: REG-PRIV-SAEJEE-2026-v6.0

TÍTULO I. PREÁMBULO ESTATUTARIO, NATURALEZA GARANTISTA DE LA CONFIDENCIALIDAD Y CUADRO DE IDENTIFICACIÓN DEL RESPONSABLE

ARTÍCULO 1.° - Objeto estatutario, alcance dogmático-jurídico y principios rectores de confidencialidad y reserva institucional

I. - La presente **Política de Confidencialidad, Secreto Profesional y Reserva Documental** (Referencia de depósito: REG-PRIV-SAEJEE-2026-v6.0) constituye el instrumento normativo interno que regula el deber de reserva, el secreto profesional académico y pericial, la confidencialidad de las comunicaciones y la seguridad criptográfica de los expedientes en **UNIVERSITÉ EUROPÉENNE DE PARIS - UNIVERSITÉ EUROPÉENNE (SAEJEE — UNIVERSIDAD EUROPEA DE PARÍS)**. Complementando de manera especializada el Estatuto de Protección de Datos Personales (PDF), el Aviso Legal e Impressum Estatutario (PDF) y las Condiciones Generales de Contratación (PDF), este cuerpo normativo establece las garantías sustantivas de intangibilidad e inviolabilidad de la información confiada por los postulantes, estudiantes de posgrado y doctorado, investigadores, miembros de tribunales examinadores y egresados internacionales.

II. - En ejercicio de su autonomía estatutaria y en observancia del artículo 32 del Reglamento (UE) 2016/679 (RGPD), la Universidad despliega su actividad bajo cuatro (4) principios rectores de aplicación transversal:

- 1° **Principio de Confidencialidad e Intangibilidad Registral:** Garantía estatutaria de que ningún expediente académico, manuscrito de investigación doctoral, deliberación de jurado examinador ni registro financiero será divulgado, comercializado o exhibido ante terceros no autorizados, preservando su integridad criptográfica durante todo su ciclo vital.

- 2° **Principio de Custodia Legítima y Finalidad Vinculada:** Todo procesamiento de información confidencial responde exclusivamente a fines de docencia superior, investigación científica de tercer ciclo, evaluación sumativa, certificación académica y verificación oficial de títulos, quedando vedado cualquier uso secundario incompatible.
- 3° **Principio de Minimización y Reserva en la Verificación Pública (Art. 5.1.c RGPD):** Delimitación estricta entre el estrato público de validación de credenciales (código QR limitado a confirmar la veracidad del diploma) y el estrato reservado del expediente analítico completo (Anexos A, B y C), cuyo acceso permanece protegido tras autenticación criptográfica.
- 4° **Principio de Transparencia y Seguridad Jurídica Transnacional:** Acceso permanente y auditable de los estudiantes e investigadores —tanto en la Unión Europea como en América Latina (LATAM) y el resto del mundo— a las normas, bases jurídicas y protocolos técnicos que amparan la confidencialidad de su acervo académico.

ARTÍCULO 2 – Cuadro sinóptico de personería jurídica, registros oficiales del Estado francés y órganos de control de confidencialidad

I. – La custodia de la información confidencial recabada en el portal institucional (www.universiteeuropeenne.paris), en el Campus Virtual (LMS) y en el sistema de verificación (https://www.saejee.eu/verification/) se ejecuta bajo la titularidad y responsabilidad directa de la entidad francesa cuyos datos registrales y órganos de control se detallan a continuación:

Atributo Estatutario / Órgano de Control	Identificador Oficial / Canal Institucional
Denominación Oficial de la Entidad	UNIVERSITÉ EUROPÉENNE DE PARIS – UNIVERSITÉ EUROPÉENNE (SAEJEE — UNIVERSIDAD EUROPEA DE PARÍS)
Personería Jurídica y Marco Estatutario	Personería jurídica, plena vigencia institucional ininterrumpida desde el **11 de junio de 1991 (35 años)** y verificación registral en los sistemas oficiales del Estado francés (data.gouv.fr / DINUM / INSEE / SIRENE) · Asociación declarada regida por la *Loi du 1er juillet 1901* (PDF) y el *Article L. 731-1 del Code de l'éducation* (PDF).
Domicilio de la Sede Social y Estatutaria	229 Boulevard Voltaire, 75011 Paris, République Française (Ficha Oficial SIRET y Mapa — PDF)
Identificadores Estatales (INSEE / SIRENE / RNA / LEI)	SIREN: 399 107 937 · SIRET: 399 107 937 00019 · NIC: 00019 · RNA: W751108902 (751P00108902) · LEI: 969500363 7S275T57497 (Certificado

Atributo Estatutario / Órgano de Control	Identificador Oficial / Canal Institucional
	INSEE – PDF · Verificación Estatal Marianne – PDF)
Clasificación NAF / APE e IVA Intracomunitario	Código NAF/APE: 94.99Z (NAF 2025: 94.99Y) · Número de IVA Intracomunitario (DGFiP): FR55399107937
Rectorado Institucional	Prof. Dr. Ramón L. Maiha Mulleras (info@universiteeuropeenne.paris)
Presidencia y Vicerrectorado Académico (CAO)	D. Ramón Segundo (cao@universiteeuropeenne.paris)
Consejería Jurídica (CLO) y Unidad PRADA	D. Manuel Santos (prada@universiteeuropeenne.paris · clo@universiteeuropeenne.paris)
Dirección de Cumplimiento Normativo (CCO)	Dña. Alicia Bejarano (cco@universiteeuropeenne.paris · communication@universiteeuropeenne.paris)
Delegación de Protección de Datos (DPO / DPD)	Unidad de Protección de Datos y Secreto Documental (dpd@universiteeuropeenne.paris)
Secretaría General Académica y Atención Directa	scolarite@saejee.eu · info@universiteeuropeenne.paris · Línea institucional y WhatsApp: +33 (7) 70 22 36 99

TÍTULO II. RÉGIMEN JURÍDICO DE LA CONFIDENCIALIDAD, TUTELA TRANSNACIONAL Y DESLINDE NORMATIVO

ARTÍCULO 3 – Convergencia del Derecho de la Unión Europea y de la República Francesa en beneficio del estudiante internacional

I. – El régimen de confidencialidad de **SAEJEE – UNIVERSITÉ EUROPÉENNE DE PARIS** otorga a todos los estudiantes, doctorandos y egresados —con especial proyección hacia los profesionales residentes en América Latina (LATAM) y el espacio iberoamericano— el nivel más elevado de tutela jurídica existente en el derecho comparado, al someter la custodia de sus expedientes de manera directa e incondicional al ordenamiento comunitario europeo y francés:

- 1° **Reglamento (UE) 2016/679 (RGPD):** De aplicación directa y preferente en cuanto al ámbito territorial (Art. 3), principios de confidencialidad

e integridad (Art. 5.1.f), bases de licitud (Arts. 6 y 9), derechos del interesado (Arts. 12 a 22), seguridad criptográfica y organizativa (Arts. 24 a 39), transferencias internacionales (Arts. 44 a 49) y garantías en investigación científica y archivo en interés público (Art. 89).

- 2° ***Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*** **(modificada):** Ley estatutaria de la República Francesa que regula la protección de los ficheros informáticos, las garantías procedimentales ante la *Commission Nationale de l'Informatique et des Libertés* (CNIL) y el régimen de dispositivos de almacenamiento en terminales (Art. 82).
- 3° **Protección del secreto profesional y de la propiedad intelectual en derecho francés:** Articulación con las normas de confidencialidad civil y deontológica y con la protección de la autoría intelectual de los trabajos de investigación doctoral (*Code de la propriété intellectuelle*, Arts. L. 111-1 y siguientes).

ARTÍCULO 4 – Deslinde dogmático-jurídico entre las atribuciones educativas francesas y la licitud del tratamiento de datos

I. – La capacidad jurídica, la autonomía pedagógica, la suscripción de convenios interuniversitarios europeos y la expedición de Diplomas Interuniversitarios de Doctorado (DIU-DOCTORAT) y Diplomas de Universidad (DU) se fundamentan en el *Code de l'éducation* (*Art. L. 151-1*, *Art. L. 613-2*, *Art. L. 731-1*, *Art. L. 444-1*, *Art. L. 444-8*, *Art. L. 718-16* y *Art. L. 123-3*) y en el *Code de la recherche* (*Art. L. 412-1*).

II. – Conforme al principio de especialidad normativa, dichas normas educativas e investigadoras consolidan la plena legitimidad institucional y académica de la Universidad en la República Francesa, mientras que cada operación sobre datos personales se sujeta de manera específica e inexcusable a las bases de licitud de los artículos 6 y 9 del RGPD, garantizando así una doble conformidad —académica y de privacidad— ante cualquier auditoría nacional o internacional.

TÍTULO III. MAPEO OPERATIVO DE CONFIDENCIALIDAD EN EL CICLO ACADÉMICO Y CRITERIOS DE OBLIGATORIEDAD

ARTÍCULO 5 – Mapeo transversal de confidencialidad en las siete fases del ciclo formativo y certificador

I. – En cumplimiento del artículo 12 del RGPD, la Universidad detalla el régimen de reserva y finalidad aplicable a cada uno de los siete (7) ámbitos operativos de su actividad institucional:

Ámbito Operativo	Categoría de Información Protegida	Fuente de Recolección	Finalidad Institucional y Régimen de Reserva
1. Navegación y Consulta Web	Identificadores técnicos de sesión (IP, *user-agent*), registros de cortafuegos y sellos de tiempo.	Automática desde el terminal del usuario al conectarse al portal seguro.	Seguridad perimetral del sitio, prevención de intrusiones y estabilidad técnica bajo protocolo TLS 1.3.
2. Admisión y Matriculación	Identidad civil, pasaporte/documento nacional, datos de contacto y títulos universitarios previos aportados.	Aportada directamente por el candidato en su dossier de admisión.	Verificación confidencial por la Comisión de Admisiones, apertura del expediente único y formalización contractual.
3. Docencia en Campus Virtual (LMS)	Credenciales individuales, progreso pedagógico, entregas de seminarios, foros académicos y tutorías.	Generada por el estudiante durante su actividad en el LMS Moodle.	Seguimiento docente reservado, evaluación continua y soporte técnico-pedagógico personalizado.
4. Evaluaciones y Tesis Doctoral (Anexos B y C)	Exámenes sumativos (escala 0–20), manuscritos de tesis doctoral, informes de codirectores y actas del *Jury de Thèse*.	Producción intelectual del doctorando y dictámenes del cuerpo examinador.	Calificación oficial del grado, protección de la propiedad intelectual del autor y custodia del acta de defensa doctoral.
5. Prácticas Periciales, Clínicas y Forenses (Anexo A)	Bitácoras procedimentales (*Logbooks*), informes de supervisión clínica/forense y cómputo de horas auditadas.	Documentada por el alumno y certificada por el tutor clínico o forense.	Acreditación del componente práctico supervisado (**57,27 %** en el modelo doctoral de referencia) con anonimización total de terceros.
6. Tesorería, Facturación y Garantías de Reembolso	Facturas, referencias de pago, identificadores de transacción PayPal y	Facilitada por el contratante y confirmada por la pasarela financiera.	Contabilidad fiscal francesa (TVA FR55399107937) y ejecución reservada

Ámbito Operativo	Categoría de Información Protegida	Fuente de Recolección	Finalidad Institucional y Régimen de Reserva
	expedientes de garantía.		de las garantías de reembolso (14, 30 y 180 días).
7. Verificación Pública de Credenciales (QR / PAdES)	Nombre del titulado, matrícula única, denominación del diploma, mención, fecha y firmas PAdES.	Asiento registral matriz consolidado en la Secretaría General.	Validación inmediata de autenticidad ante autoridades, cancillerías y empleadores en https://www.saejee.eu/verification/.

ARTÍCULO 6 – Ponderación de bases jurídicas de licitud y consecuencias de la obligatoriedad documental

I. – La reserva y legitimidad de los ámbitos operativos descritos en el Artículo 5 descansan sobre cuatro (4) fundamentos jurídicos específicos del artículo 6.1 del RGPD:

- 1° **Ejecución del contrato formativo (Art. 6.1.b RGPD):** Ampara la admisión, matriculación, docencia en el Campus Virtual, tutoría de tesis, evaluación sumativa y expedición del Diploma y del Suplemento Europeo al Título (SET).
- 2° **Cumplimiento de obligaciones legales (Art. 6.1.c RGPD):** Ampara la teneduría de libros contables y fiscales exigida por el *Code de commerce* (Art. L. 123-22) y el *Code général des impôts* durante diez (10) años, así como la custodia estatutaria de las actas oficiales de grado.
- 3° **Interés legítimo institucional ponderado (Art. 6.1.f RGPD):** Ampara la seguridad lógica de los servidores europeos y la operación permanente del portal de verificación criptográfica (https://www.saejee.eu/verification/) para proteger tanto a la Universidad como al propio graduado frente a la falsificación o usurpación de títulos académicos.
- 4° **Consentimiento expreso e informado (Art. 6.1.a RGPD):** Requerido exclusivamente para las cookies no esenciales de análisis o personalización y para las comunicaciones informativas opcionales.

II. – *Consecuencias jurídicas de la falta de aportación de datos obligatorios:* Dado que la identidad fehaciente del alumno, sus antecedentes académicos de ingreso y su regularidad arancelaria son presupuestos esenciales de validez de toda titulación universitaria, la negativa a suministrar los datos marcados como obligatorios conlleva de pleno derecho: *a)* la imposibilidad de formalizar la admisión o matrícula; *b)* la suspensión preventiva de las credenciales del Campus Virtual; y *c)*

la imposibilidad legal de expedir diplomas, certificados o Suplementos Europeos al Título.

TÍTULO IV. TRATAMIENTO DE INFORMACIÓN SENSIBLE, SEPARACIÓN INFRANQUEABLE DE EXPEDIENTES Y SECRETO PROFESIONAL PERPETUO

ARTÍCULO 7 – Separación categórica entre el expediente académico del estudiante y los registros clínicos, neuropsicológicos o judiciales de terceros (Logbook)

I. – En los programas superiores de posgrado y doctorado vinculados a las Ciencias de la Salud, Psicología Criminal, Neuropsicología Clínica, Psiquiatría Forense, Neuropunición y Ciencias Jurídicas y Forenses, la Universidad impone una **frontera técnica y jurídica infranqueable** entre el expediente académico-administrativo del estudiante y la información sensible de terceros analizada durante la práctica supervisada:

- 1° **Regla de separación absoluta de servidores y legajos:** El expediente académico del alumno (integrado por sus datos identificativos, matrícula, calificaciones y actas) se custodia en el registro central de la Secretaría General. Por el contrario, las historias clínicas, protocolos psicodiagnósticos, peritajes judiciales, declaraciones de víctimas o expedientes penales que el doctorando examine en hospitales, clínicas, tribunales o centros penitenciarios durante sus prácticas supervisadas **jamás se incorporan en bruto ni con datos identificativos de terceros a los servidores de la Universidad ni al expediente personal del alumno.**
- 2° **Cumplimiento concurrente de los artículos 6, 9 y 10 del RGPD en la actividad investigadora:** Toda actividad de investigación o práctica pericial que verse sobre datos relativos a la salud (Art. 9 RGPD) o sobre datos de infracciones y condenas penales (Art. 10 RGPD) se sujeta en su centro de origen al consentimiento explícito del paciente o evaluado (Art. 9.2.a RGPD) o a las garantías de investigación científica y archivo en interés público (Art. 9.2.j y Art. 89.1 RGPD), verificadas por el comité de ética o la autoridad judicial competente.
- 3° **Cláusula de intangibilidad frente a accesos no autorizados:** La condición de estudiante, docente o investigador de **SAEJEE — UNIVERSITÉ EUROPÉENNE DE PARIS** no faculta en ningún caso para extraer, copiar o difundir datos nominales de pacientes o justiciables fuera de los recintos clínicos o judiciales donde se desarrolle la práctica auditada.

ARTÍCULO 8 – Protocolos científicos internacionales (PRISMA / ICH-GCP), anonimización en origen y deber perpetuo de secreto profesional

I. – Para la validación de las memorias de práctica supervisada (Anexo A – *Logbook*) y de las tesis doctorales (Anexo C) conforme al artículo 89 del RGPD y al *Article L. 412-1 del Code de la recherche* (PDF), son de cumplimiento obligatorio las siguientes tres (3) salvaguardas metodológicas y deontológicas:

- 1° **Anonimización irreversible en fase de campo:** Antes de consignar cualquier caso clínico, evaluación neuropsicológica o dictamen pericial en el *Logbook* (Anexo A) o en el manuscrito de tesis (Anexo C), el doctorando debe aplicar técnicas de disociación definitiva que eliminen todo identificador directo o indirecto, garantizando que únicamente se procesen variables estadísticas, clínicas o jurídicas completamente anonimizadas.
- 2° **Rigor metodológico internacional (*PRISMA* e *ICH-GCP*):** Las investigaciones sistemáticas, metaanálisis y estudios clínicos o forenses se estructuran bajo las directrices internacionales **PRISMA** (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), las normas de Buena Práctica Clínica **ICH-GCP** y los principios éticos de la Declaración de Helsinki.
- 3° **Deber perpetuo de secreto profesional (*Secret professionnel*):** Todo miembro del cuerpo docente, director de tesis, integrante de tribunal examinador, personal administrativo y estudiante matriculado queda sujeto a un deber estricto e incondicional de secreto profesional respecto de toda información reservada o pericial conocida con ocasión de su actividad académica, obligación que subsiste a perpetuidad aun después de concluida su vinculación con la Universidad.

TÍTULO V. CUSTODIA FÍSICA Y LÓGICA, AUDITORÍA DE VERIFICACIÓN QR Y DESLINDE TÉCNICO ENTRE LEGALIZACIÓN INTERNACIONAL Y CIBERSEGURIDAD

ARTÍCULO 9 – Resguardo físico y digital de actas, minimización en la plataforma QR y registro auditable de consultas (Logs)

I. – La Universidad aplica un protocolo de doble custodia –física y criptográfica– sobre los expedientes de titulación:

- 1° **Trazabilidad e inmutabilidad de las actas de calificación:** El acceso al repositorio matriz de calificaciones y expedientes se restringe bajo

el principio de necesidad de conocimiento (*need-to-know principle*). Toda inscripción o rectificación material en un acta académica requiere resolución formal refrendada por el Rectorado o la Secretaría General, conservándose un registro histórico inalterable de auditoría.

- 2° **Reserva frente a terceros:** Ningún expediente académico completo es entregado o exhibido a terceros ajenos al titular sin que medie: *a)* autorización escrita e inequívoca del propio estudiante o graduado; o *b)* requerimiento legal, notarial o judicial expedido por autoridad competente.

II. - La plataforma oficial de verificación documental (https://www.saejee.eu/verification/) conjuga la transparencia registral frente a autoridades y empleadores con la protección de la intimidad del graduado mediante tres (3) reglas técnicas:

- *a)* **Respuesta pública estrictamente acotada:** El escaneo del código QR impreso en el Diploma o en el Resumen Académico (SET) devuelve únicamente los metadatos registrales indispensables para certificar la legitimidad del título: nombre y apellidos del titular, número de matrícula institucional, denominación oficial del grado obtenido, fecha de expedición, mención y validez de las firmas criptográficas PAdES.
- *b)* **Reserva absoluta de los anexos analíticos desglosados:** En cumplimiento del principio de minimización (Art. 5.1.c RGPD), la consulta pública abierta jamás expone el documento de identidad, el domicilio particular, las calificaciones pormenorizadas asignatura por asignatura del Anexo B ni los registros detallados de los Anexos A y C, cuyo cotejo íntegro requiere las credenciales de verificación autorizada (ESIGNACT / ESIGN-UETA) suministradas por el propio graduado a la autoridad evaluadora.
- *c)* **Bitácora de auditoría antifraude (*Audit Logs*):** Cada consulta efectuada en la plataforma de verificación genera un asiento técnico de seguridad (dirección IP consultante, sello de tiempo exacto e identificador de certificado consultado) con el único propósito de garantizar la trazabilidad pericial y detectar cualquier tentativa de uso fraudulento o alteración documental.

ARTÍCULO 10 – Matriz de deslinde técnico y jurídico entre los instrumentos de autenticación internacional y las medidas de ciberseguridad RGPD

I. - A efectos de proporcionar claridad técnica absoluta a los comités de evaluación, peritos informáticos y auditores legales, la Universidad establece la distinción funcional y la complementariedad entre los mecanismos de autenticación documental física/internacional (aplicados en los títulos de formato **A3 — 420 × 297 mm** con doble sello seco en relieve *gaufrage à sec* y hologramas ópticamente variables) y los controles de ciberseguridad lógica del artículo 32 del RGPD:

Instrumento de Autenticación Documental	Alcance Jurídico y Probatorio Real	Control Paralelo de Ciberseguridad y Privacidad (Art. 32 RGPD)
1. Apostilla del Convenio de La Haya de 5 de octubre de 1961 (sobre el título o en *allonge*)	Autentica en el tráfico jurídico internacional la veracidad de la firma de la autoridad pública o fedatario interviniente, la calidad en que ha actuado y la identidad del sello o timbre oficial.	La Apostilla certifica la cadena de firmas públicas del documento; de forma paralela e independiente, la protección de los datos personales en red se asegura mediante cifrado TLS 1.3, bases de datos cifradas (AES-256) y control de accesos lógicos en la Unión Europea.
2. Firma Electrónica Avanzada y Sellado de Tiempo (PAdES / Reglamento eIDAS UE 910/2014)	Garantiza la autenticidad del origen, el no repudio y la integridad criptográfica bit a bit del documento electrónico en formato PDF, invalidando automáticamente cualquier alteración ulterior.	Protege la inmutabilidad del archivo PDF expedido, complementándose en los servidores de **OVHcloud SAS** y **Hetzner Online GmbH** con copias de seguridad georredundantes, cortafuegos de aplicación web (*WAF*) y monitoreo continuo.
3. Certificación Notarial Europea y Seguridades Físicas A3 (doble sello seco y hologramas)	Da fe de la legitimación de firmas autógrafas, de la fecha cierta de expedición y de la inviolabilidad física del soporte cartular en formato A3 (420 × 297 mm).	Opera sobre el soporte físico y fedatario, mientras que la licitud del tratamiento de los datos del graduado descansa sobre el artículo 6.1.b/c/f del RGPD y la custodia restringida en la Secretaría General.

TÍTULO VI. GOBERNANZA DE ENCARGADOS, TRANSFERENCIAS TRANSFRONTERIZAS Y PROTOCOLOS DE BLOQUEO Y PURGA DOCUMENTAL

ARTÍCULO 11 – Contratos de encargo de tratamiento (DPA Art. 28 RGPD), soberanía de alojamiento europeo y matriz de transferencias internacionales

I. – La cadena de confidencialidad con proveedores tecnológicos e instituciones académicas aliadas se estructura bajo tres (3) niveles de

blindaje contractual:

- 1° **Acuerdos vinculantes con Encargados del Tratamiento (Art. 28 RGPD):** El alojamiento del Campus Virtual (LMS), las bases de datos registrales y el sistema de correo institucional se encuentran íntegramente radicados en la Unión Europea a través de **OVHcloud SAS** (2 rue Kellermann, 59100 Roubaix, Francia — centros de datos en París, Roubaix y Gravelines) y **Hetzner Online GmbH** (Industriestr. 25, 91710 Gunzenhausen, Alemania), sujetos a contratos *DPA* que prohíben toda subcontratación no autorizada o transferencia subrepticia fuera del Espacio Económico Europeo.
- 2° **Acuerdos de Corresponsabilidad Interuniversitaria (Art. 26 RGPD):** En el marco de los convenios de cooperación interuniversitaria suscritos conforme al *Article L. 718-16 del Code de l'éducation* con **Helmstedt University** (Alemania) y **Universitätsmedizin Berlin** (Alemania), el tratamiento de las actas de cotutela y evaluación conjunta se rige por acuerdos transparentes de corresponsabilidad bajo jurisdicción comunitaria europea.
- 3° **Matriz regional de garantías para flujos transfronterizos fuera del EEE (Arts. 45, 46 y 49 RGPD):**

Región o Jurisdicción de Destino	Categoría de Destinatarios	Mecanismo Jurídico de Garantía (RGPD)	Canal Interno de Verificación y Consulta
América Latina (LATAM) e Iberoamérica	Estudiantes matriculados, tutores clínicos/periciales locales y autoridades ministeriales de reconocimiento requeridas por el graduado.	Cláusulas Contractuales Tipo de la Comisión Europea (SCC Decisión UE 2021/914 — Art. 46.2.c RGPD) + cifrado TLS 1.3 / AES-256, o excepciones tasadas de ejecución contractual y defensa de derechos en trámites de reconocimiento (Arts. 49.1.b y 49.1.e RGPD).	Solicitud directa ante la Unidad Jurídica PRADA: prada@universiteeuropeenne.paris.
Espacio Económico Europeo, Reino Unido y Suiza	Universidades europeas en convenio, notarios europeos y evaluadores académicos.	Libre circulación dentro del EEE (Art. 1.3 RGPD) o Decisiones de Adecuación vigentes (Art. 45 RGPD).	Supervisión directa por la Delegación de Protección de Datos: dpd@universiteeuropeenne.paris.

Región o Jurisdicción de Destino	Categoría de Destinatarios	Mecanismo Jurídico de Garantía (RGPD)	Canal Interno de Verificación y Consulta
Otros Terceros Países	Entidades empleadoras, colegios profesionales o cancillerías designadas por el propio titulado.	Ejecución de medidas a petición del interesado (Art. 49.1.b), consentimiento explícito (Art. 49.1.a) o reconocimiento de derechos (Art. 49.1.e RGPD).	Validación previa en Secretaría General: scolarite@saejee.eu.

ARTÍCULO 12 – Protocolos de bloqueo preventivo, sobrescritura segura (Data Wiping) y preservación histórica

I. – En concordancia con la matriz de plazos de conservación establecida en el Artículo 12 del Estatuto de Protección de Datos Personales (conservación **permanente** de actas de grado, diplomas y SET en el archivo histórico restringido; **10 años** para la documentación fiscal y contable bajo el *Art. L. 123-22 del Code de commerce*; **5 años** para actuaciones PRADA; **3 años** para consultas de admisión sin matrícula; y **12 meses** para registros técnicos de conexión), la extinción del plazo aplicable a los datos no permanentes activa un protocolo técnico en tres (3) etapas:

- 1° **Bloqueo lógico preventivo:** Restricción inmediata de visibilidad en los sistemas operativos ordinarios, manteniendo los registros bloqueados únicamente a disposición de autoridades judiciales o administrativas hasta la prescripción de eventuales acciones legales.
- 2° **Supresión criptográfica y sobrescritura segura (*Data Wiping*):** Eliminación irreversible de los soportes primarios y de respaldo mediante algoritmos de sobrescritura multipaso que impiden toda recuperación física o forense de los datos expirados.
- 3° **Preservación estadística anonimizada:** Conservación exclusiva de indicadores académicos agregados y completamente disociados para fines de memoria institucional e investigación educativa conforme al artículo 89 del RGPD.

TÍTULO VII. PROTOCOLO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD (ARTS. 33 Y 34 RGPD), MATRIZ DE COOKIES Y VIGENCIA ESTATUTARIA

ARTÍCULO 13 - Protocolo operativo en cinco pasos ante incidentes de ciberseguridad y brechas de datos personales (Data Breaches)

I. - Sin perjuicio del ejercicio gratuito y permanente de los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición (Arts. 15 a 22 RGPD) a través de los canales prada@universiteeuropeenne.paris y dpd@universiteeuropeenne.paris (con resolución en el plazo máximo de **un mes**), la Universidad mantiene un **Protocolo Operativo de Respuesta ante Incidentes y Brechas de Seguridad** en estricto cumplimiento de los artículos 33 y 34 del RGPD:

- 1° **Paso 1 — Detección, alerta temprana y contención técnica inmediata:** Ante cualquier anomalía o tentativa de intrusión detectada por los sistemas de monitoreo, la Dirección de Tecnologías de la Información y Sistemas (cio@universiteeuropeenne.paris) ejecuta el aislamiento inmediato del segmento afectado, la revocación preventiva de tokens de sesión y la preservación forense de las bitácoras de servidor.
- 2° **Paso 2 — Evaluación jurídico-técnica de severidad y riesgo:** De forma conjunta, la Consejería Jurídica PRADA (prada@universiteeuropeenne.paris), la Dirección de Cumplimiento (cco@universiteeuropeenne.paris) y la Delegación de Protección de Datos (dpd@universiteeuropeenne.paris) evalúan la naturaleza del incidente, las categorías de datos involucradas y la eficacia del cifrado previo (AES-256) para determinar el nivel de riesgo para los derechos y libertades de los titulares.
- 3° **Paso 3 — Notificación reglada a la Autoridad de Control en un máximo de 72 horas (Art. 33 RGPD):** Si el incidente entraña un riesgo para los derechos y libertades de las personas físicas, el Responsable del Tratamiento formaliza la notificación oficial ante la *Commission Nationale de l'Informatique et des Libertés* (CNIL) sin dilación indebida y, a más tardar, dentro del plazo improrrogable de **setenta y dos (72) horas** desde que se tuvo constancia de la brecha.
- 4° **Paso 4 — Comunicación transparente a los titulares afectados (Art. 34 RGPD):** Cuando sea probable que la violación de seguridad entrañe un **alto riesgo** para los derechos y libertades de los interesados, la Universidad se lo comunica directamente en lenguaje claro y sencillo, informando de las medidas adoptadas y de las recomendaciones de seguridad pertinentes.
- 5° **Paso 5 — Remediación estructural y asiento en el Libro Registro de Incidentes (Art. 33.5 RGPD):** Documentación exhaustiva de los hechos, sus

efectos y las medidas correctivas implantadas en el registro interno de auditoría de seguridad de la institución.

ARTÍCULO 14 – Matriz técnica de dispositivos de seguimiento (Cookies), segregación de comunicaciones y sello de vigencia institucional

I. – En aplicación del artículo 82 de la *Loi n° 78-17 Informatique et Libertés* y de las directrices de la CNIL, los dispositivos de almacenamiento y recuperación de datos en equipos terminales utilizados en el ecosistema digital de la Universidad se rigen por la siguiente matriz técnica:

Categoría de Dispositivo / Cookie	Finalidad Técnica y Operativa	Régimen Legal de Consentimiento (Art. 82 Loi 78-17)	Plazo Máximo de Expiración
1. Estrictamente Necesarias y de Seguridad Transaccional	Autenticación de sesión en el Campus Virtual (LMS Moodle), equilibrio de carga, prevención de fraude CSRF y vinculación segura con la pasarela financiera bajo la identidad fiscal FR55399107937 (amparada por la Protección al Comprador de PayPal de 180 días).	**Exentas de consentimiento previo** por ser estrictamente indispensables para la prestación del servicio expresamente solicitado por el usuario.	Sesión activa (y hasta un máximo técnico de 12 meses para tokens de seguridad).
2. Medición de Audiencia y Analítica Estadística	Medición agregada y anónima del rendimiento de las páginas académicas para optimizar la arquitectura documental del portal.	**Sujetas a consentimiento previo, libre y específico** mediante banner simétrico con botones de idéntica jerarquía para aceptar o rechazar.	Máximo de trece (13) meses conforme a los criterios de la CNIL.
3. Funcionalidad y Preferencias Lingüísticas	Conservación del idioma de lectura seleccionado por el usuario (FR / ES / EN) y preferencias de accesibilidad visual.	**Sujetas a consentimiento previo** cuando excedan de la sesión activa del navegador.	De seis (6) a doce (12) meses, revocable en cualquier momento desde el pie de página.

II. – *Segregación estricta entre comunicaciones académicas y comunicaciones informativas:*

- *a)* **Comunicaciones académico-administrativas obligatorias (Art. 6.1.b RGPD):** Las notificaciones sobre estado de matrícula, tutorías, convocatorias de examen, defensa de tesis, expedición de diplomas o garantías contractuales forman parte esencial de la ejecución del contrato educativo y se remiten a través de los dominios oficiales @universiteeuropeenne.paris y @saejee.eu.
- *b)* **Comunicaciones informativas sobre nueva oferta de posgrado (Art. 6.1.a RGPD):** Se remiten exclusivamente a quienes hayan otorgado su autorización expresa e incorporan en cada envío un mecanismo inmediato y gratuito de baja automatizada (*opt-out*).

III. - *Vigencia y depósito estatutario:* La presente **Política de Confidencialidad, Secreto Profesional y Reserva Documental** (Versión consolidada v6.0 — 2026 · Referencia de depósito institucional: REG-PRIV-SAEJEE-2026-v6.0), aprobada por el Rectorado Institucional de **UNIVERSITÉ EUROPÉENNE DE PARIS - UNIVERSITÉ EUROPÉENNE (SAEJEE — UNIVERSIDAD EUROPEA DE PARÍS)** bajo la firma del **Prof. Dr. Ramón L. Maiha Mulleras** en París (229 Boulevard Voltaire, 75011 Paris, République Française), se encuentra en pleno vigor y armonizada con el Aviso Legal e Impressum Estatutario, las Condiciones Generales de Contratación y el Estatuto de Protección de Datos Personales.