

SECCIÓN 1 - DESCRIPCIÓN DEL TRATAMIENTO DE DATOS PERSONALES

1. LOS DATOS PERSONALES QUE SERÁN PROCESADOS:

Producto	Los datos personales que pueden procesarse pueden incluir:	A quién puede pertenecer:
Unit4 ERP x	Nombres; direcciones; detalles del contrato; números de teléfono (incluido el móvil); correos electrónicos); otra información de contacto; fecha de nacimiento; edad; lugar de nacimiento; Nacionalidad o ciudadanía; residencia; domicilio; lenguajes hablados); número de pasaporte; número de seguridad nacional o número de seguridad social o referencia de la tarjeta de identificación; estado civil; detalles del beneficiario bajo beneficios; género; información laboral (incluyendo: salario; puesto; escala salarial; escalón salarial; competencias y notas personales); Información sobre los impuestos; información sobre beneficios; Membresía de la unión; pariente más cercano proporcionado (nombre; dirección; fecha de nacimiento; número de teléfono; detalles de contacto de emergencia); fechas de inicio y finalización del empleo; detalles de la cuenta bancaria o de la tarjeta de crédito; datos de la empresa de servicios personales (nombre, número de registro y domicilio social); cargos de dirección; Números de IVA; documentos (escritos o electrónicos) que contengan cualquiera de los anteriores.	Empleados actuales o anteriores; Contratistas o subcontratistas (de cualquier variedad), agentes o administradores; y Solicitantes o posibles empleados.
Unit4 ERP 7	Nombres; direcciones; detalles del contrato; números de teléfono (incluido el móvil); correos electrónicos); otra información de contacto; fecha de nacimiento; edad; lugar de nacimiento; Nacionalidad o ciudadanía; residencia; domicilio; lenguajes hablados); número de pasaporte; número de seguridad nacional o número de seguridad social o referencia de la tarjeta de identificación; estado civil; detalles del beneficiario bajo beneficios; género; información laboral (incluyendo: salario; puesto; escala salarial; escalón salarial; competencias y notas personales); Información sobre los impuestos; información sobre beneficios; Membresía de la unión; pariente más cercano proporcionado (nombre; dirección; fecha de nacimiento; número de teléfono; detalles de contacto de emergencia); fechas de inicio y finalización del empleo; detalles de la cuenta bancaria o de la tarjeta de crédito; datos de la empresa de servicios personales (nombre, número de registro y domicilio social); cargos de dirección; Números de IVA; documentos (escritos o electrónicos) que contengan cualquiera de los anteriores.	Empleados actuales o anteriores; Contratistas o subcontratistas (de cualquier variedad), agentes o administradores; y Solicitantes o posibles empleados.
Unit4 Financials	Nombres; direcciones; detalles del contrato; números de teléfono (incluido el móvil); correos electrónicos); otra información de contacto; fecha de nacimiento; edad; lugar de nacimiento; Nacionalidad o ciudadanía; residencia; domicilio; lenguajes hablados); número de pasaporte; número de seguridad nacional o número de seguridad social o referencia de la tarjeta de identificación; estado civil; detalles del beneficiario bajo beneficios; género; información laboral (incluyendo: salario; puesto; escala salarial; escalón salarial; competencias y notas personales); Información sobre los impuestos; información sobre beneficios; Membresía de la unión; pariente más cercano proporcionado (nombre; dirección; fecha de nacimiento; número de teléfono; detalles de contacto de emergencia); fechas de inicio y finalización del empleo; detalles de la cuenta bancaria o de la tarjeta de crédito; datos de la empresa de servicios personales (nombre, número de registro y domicilio social); cargos de dirección; Números de IVA; documentos (escritos o electrónicos) que contengan cualquiera de los anteriores.	Empleados actuales o anteriores; Contratistas o subcontratistas (de cualquier variedad), agentes o administradores; y Solicitantes o posibles empleados.
Unit4 Student Management	<p>Nombres; direcciones; detalles del contrato; números de teléfono (incluido el móvil); correos electrónicos); otra información de contacto; fecha de nacimiento; edad; lugar de nacimiento; Nacionalidad o ciudadanía; residencia; domicilio; lenguajes hablados); número de pasaporte; número de seguridad nacional o número de seguridad social o referencia de la tarjeta de identificación; estado civil; detalles del beneficiario bajo beneficios; género; información laboral (incluyendo: salario; puesto; escala salarial; escalón salarial; competencias y notas personales); Información sobre los impuestos; información sobre beneficios; Membresía de la unión; pariente más cercano proporcionado (nombre; dirección; fecha de nacimiento; número de teléfono; detalles de contacto de emergencia); fechas de inicio y finalización del empleo; detalles de la cuenta bancaria o de la tarjeta de crédito; datos de la empresa de servicios personales (nombre, número de registro y domicilio social); cargos de dirección; Números de IVA; documentos (escritos o electrónicos) que contengan cualquiera de los anteriores.</p> <p>Datos personales adicionales para empleados anteriores y actuales: tipo de personal (p. Ej., Facultad, asesor, director de vivienda); Departamento académico; estado de contratación; Estado de Empleo; carga de trabajo; rango de la facultad; publicaciones; seguimiento del estado del trabajo; detalles de educación y detalles de calificación.</p> <p>Datos personales adicionales para solicitantes anteriores y actuales: información universitaria anterior; transcripciones y / o resultados de pruebas (adicionales); estado de salud física; cartas de antiguos empleadores; e información sobre el lugar de trabajo.</p> <p>Datos personales adicionales para estudiantes anteriores y actuales: expediente académico que incluye resultados y metas; detalles de inscripción; detalles de la progresión académica (incluidas las calificaciones); archivos académicos; colocaciones académicas o laborales; detalles de planificación del curso; historial de facturación y pagos; preferencias e historia de vivienda; detalles de la ayuda financiera; historial médico (incluidas vacunas, alergias, afecciones médicas), información del seguro y documentación médica.</p>	Empleados actuales o anteriores (incluidos los profesores o el personal); Contratistas o subcontratistas (de cualquier variedad), agentes o directores; Solicitantes o posibles empleados; y Estudiantes actuales, anteriores y futuros.
Unit4 FP&A	Nombres; direcciones; números de teléfono (incluido el móvil); correos electrónicos); otra información de contacto. No es necesario almacenar o procesar otros datos personales para lograr los objetivos del producto (como se establece a continuación), pero el producto puede almacenar o procesar otros datos personales si está configurado de tal manera que lo haga (p. Ej. datos salariales) o el Cliente lo introduce en el Producto.	Empleados actuales o anteriores; Subcontratistas (de cualquier tipo), agentes o administradores.
Unit4 Assistance PSA Suite	Nombres; direcciones; números de teléfono (incluido el móvil); correos electrónicos); otra información de contacto. No es necesario almacenar o procesar otros datos personales para lograr los objetivos del producto (como se establece a continuación), pero el producto puede almacenar o procesar otros datos personales si está configurado de tal manera para hacerlo o si introducido en el Producto por el Cliente.	Empleados actuales o anteriores; Subcontratistas (de cualquier tipo), agentes o administradores; Cualquier otra persona que sea miembro de un equipo de proyecto

		(incluidos los no empleados) solicitantes o posibles empleados. Contactos de clientes del cliente y contactos de proveedores.
Unit4 Talent Management	Nombres; direcciones; detalles del contrato; números de teléfono (incluido el móvil); correos electrónicos); otra información de contacto (dirección postal y país); fecha de nacimiento; edad; lugar de nacimiento; título profesional; Departamento. Mediante el uso del módulo Learn: inscripciones a cursos; inscripciones a sesiones; resultados de pruebas y revisiones; datos de participación de video; datos de participación de diapositivas; datos de interacción de texto; insignias y certificaciones. Mediante el uso del módulo de ejecución: datos de registro; Datos OKR; comentarios y elogios. Mediante el uso del módulo Engage: respuestas y comentarios sobre preguntas de compromiso.	Empleados actuales o anteriores; Candidatos de trabajo actuales o anteriores; Contratistas o subcontratistas (de cualquier variedad), agentes o administradores; y Solicitantes o posibles empleados.
Servicios de plataforma de personas ("PPS"), Servicios de Localización y Apps de Unit4	Dado que los PPS, los Servicios de Localización y/o las Apps de Unit4 son servicios que funcionan e interactúan con otros Productos o Servicios de Unit4, pueden procesar cualquiera o todos los tipos de Datos Personales establecidos en esta tabla en relación con los Productos y Servicios enumerados. Además, Wanda puede procesar: Unit4Id (que identifica al usuario de IDS); cualquier dato personal o información enviada por el usuario en una aplicación a la que Wanda puede estar conectada (dicha información se procesa o almacena a menos que el usuario elija que se elimine); cualquier otro dato de conversación y diálogo; metadatos cuando sean asignables a un individuo; y registros de Application Insights (un servicio de Microsoft utilizado para realizar diagnósticos).	Todas las categorías de personas enumeradas en esta tabla. Dependiendo de la aplicación o servicio al que Wanda esté conectado, el PPS podría potencialmente Procesar Datos Personales relacionados con cualquier individuo vivo que el Usuario decida enviar.
Unit4 Property Management	Nombres; direcciones; números de teléfono (incluido el móvil); dirección de correo electrónico; dirección de la página de inicio; documento nacional de identidad, NIE o número de la seguridad social; fecha de nacimiento; identidad del cliente; idioma; marcado de identidad protegida; marcado de finca; Números de IVA; información de las personas de contacto (incluyendo: título / puesto, intereses); detalles de cuenta bancaria; información de empleo (incluyendo: empleador, información de dirección); detalles del solicitante (que incluyen: profesión, ingresos anuales, año de empleo, número de personas en el hogar, propietario anterior, evaluación del informe crediticio, fecha de la evaluación crediticia); solicitante y otros atributos (definidos por el responsable del tratamiento); posición en la cola; membresía (que incluye: número de miembro, estado, fecha de inicio / finalización de la membresía, motivo de la entrada / renuncia, fecha de la primera entrada, membresía principal, membresía relacionada, puntos de arrendamiento, puntos de ahorro para el hogar); roles / categorías de personas; Usuarios (identificación de usuario, tipo de usuario, firma); Detalles del contrato de arrendamiento y propiedad del inquilino (que incluyen: identidad del destinatario de la factura para la factura electrónica, depósito de información del mandato, garantía); información de gestión de casos; contratista (asignaciones para enviar por correo); Notas (registradas por el responsable del tratamiento); documentos (escritos o electrónicos) que contengan cualquiera de los anteriores.	Empleados actuales o anteriores; Contratistas o subcontratistas (de cualquier variedad), agentes o administradores; y Solicitantes o posibles empleados; consumidores (por ejemplo, propietarios e inquilinos) de servicios de gestión.

2. NATURALEZA Y OBJETIVO (S) DEL TRATAMIENTO:

En general, la naturaleza del procesamiento por parte del encargado solo será la necesaria para permitirle cumplir con sus obligaciones y ejercer sus derechos en virtud del Acuerdo, incluida (en relación con los datos personales) la recopilación, el registro, la organización, la estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión o puesta a disposición, alineación o combinación, restricción, borrado o destrucción. El objetivo o propósito del Procesamiento es el cumplimiento de las obligaciones del Encargado y el ejercicio de sus derechos en virtud de este Acuerdo, incluido el desempeño de las funciones requeridas o solicitadas por el Responsable para el cumplimiento por parte del Responsable de sus obligaciones legales y / o contractuales. En relación y dependiendo del Producto o Servicio, el Procesamiento incluirá lo siguiente:

Producto	Naturaleza y objetivo del procesamiento
Unit4 ERP x	<p>Los Datos Personales se ingresarán en Unit4 ERP 8 para permitir al Cliente organizar y administrar los procesos relacionados con el funcionamiento operativo y la gestión y / o procesos administrativos de su negocio interno. Los procesos pueden incluir:</p> <ul style="list-style-type: none"> • Solicitudes de viaje; • Procesamiento de notas de gastos; • Procesamiento de hojas de horas; • Gestión de ausencias; • Procesos relacionados con RR.HH. y nómina: • Nómina; • Inscripción a cursos; • Gestión de competencias; • Evaluaciones; • Revisión salarial; • Registro de solicitantes; • Procesos de pago; • Facturación; • Requisitos de compra; • Planificación de Personas / Proyectos. <p>El procesamiento implicará:</p> <p>Producto (solución de software)</p>

	<p>Unit4 ERP 8 ejecuta código de software programable para que las actividades expuestas (arriba) puedan tener lugar. Esto puede implicar la transferencia de datos hacia o desde soluciones de terceros que no están bajo el control del Encargado a través de integraciones.</p> <p>Servicios</p> <p>Transferencia y almacenamiento de Datos Personales para proporcionar Servicios adicionales como se establece con más detalle en la Descripción del Servicio o en la Descripción del Servicio de la Plataforma de Personas, cuando corresponda.</p> <p>Acceso a los Datos Personales para proporcionar soporte y mantenimiento del Producto Unit4 y ayudar al Cliente en el funcionamiento de la solución como se establece con más detalle en los Términos de Soporte de Unit4.</p> <p>Acceso a los Datos personales para proporcionar configuración y / o personalización y / o migración de datos (por ejemplo, de sus sistemas heredados) y / u otros Servicios profesionales adquiridos por el Cliente.</p>
Unit4 ERP 7	<p>Los Datos Personales se ingresarán en Unit4 ERP 7 para permitir al Cliente organizar y administrar los procesos relacionados con el funcionamiento operativo y la gestión y / o procesos administrativos de su negocio interno. Los procesos pueden incluir:</p> <ul style="list-style-type: none"> • Solicitudes de viaje; • Procesamiento de hojas de horas; • Gestión de ausencias; • Procesos relacionados con RR.HH. y nómina: • Nómina; • Inscripción a cursos; • Gestión de competencias; • Evaluaciones; • Revisión salarial; • Registro de solicitantes; • Procesos de pago; • Facturación; • Requisitos de compra; • Planificación de Personas / Proyectos. <p>El procesamiento implicará:</p> <p>Producto (solución de software)</p> <p>Unit4 ERP 7 ejecuta código de software programable para que las actividades expuestas (arriba) puedan tener lugar. Esto puede implicar la transferencia de datos hacia o desde soluciones de terceros que no están bajo el control del Encargado a través de integraciones.</p> <p>Servicios</p> <p>Transferencia y almacenamiento de Datos Personales para proporcionar Servicios adicionales como se establece con más detalle en la Descripción del Servicio o en la Descripción del Servicio de la Plataforma de Personas, cuando corresponda.</p> <p>Acceso a los Datos Personales para proporcionar soporte y mantenimiento del Producto Unit4 y ayudar al Cliente en el funcionamiento de la solución como se establece con más detalle en los Términos de Soporte de Unit4.</p> <p>Acceso a los Datos personales para proporcionar configuración y / o personalización y / o migración de datos (por ejemplo, de sus sistemas heredados) y / u otros Servicios profesionales adquiridos por el Cliente.</p>
Unit4 Financials	<p>Los Datos Personales se ingresarán en Unit4 Financials para permitir al Cliente organizar y administrar los procesos relacionados con el funcionamiento operativo y la gestión y / o procesos administrativos de su negocio interno. Los procesos pueden incluir:</p> <ul style="list-style-type: none"> • Registro de cliente / proveedor / empleado; • Procesos de pago; • Facturación; • Procesamiento de notas de gastos; • Solicitudes de viaje; • Solicitudes de compra y pedidos; • Planificación de personas / proyectos; • Procesos relacionados con recursos humanos y nómina: • Nómina; • Procesamiento de hojas de horas; • Gestión de ausencias • Inscripción a cursos; • Gestión de competencias; • Evaluaciones; • Revisión salarial; • Registro de solicitantes; <p>El procesamiento implicará:</p> <p>Producto (solución de software)</p> <p>Unit4 Financials ejecuta código de software programable para garantizar que las actividades establecidas (como se detalla anteriormente) puedan llevarse a cabo. Esto puede implicar la transferencia de datos hacia o desde soluciones de terceros que no están bajo el control del Encargado a través de integraciones.</p> <p>Servicios</p> <p>Transferencia y almacenamiento de Datos Personales para proporcionar Servicios adicionales como se establece con más detalle en la Descripción del Servicio o en la Descripción del Servicio de la Plataforma de Personas correspondiente.</p>

	<p>Acceso a los Datos personales para brindar soporte y mantenimiento del Producto de Unit4 y ayudar al cliente en el funcionamiento de la solución como se establece con más detalle en los Términos de soporte de Unit4.</p> <p>Acceso a los Datos personales para proporcionar configuración y / o personalización y / o migración de datos (por ejemplo, de sus sistemas heredados) y / u otros Servicios profesionales adquiridos por el Cliente.</p>
Unit4 Student Management	<p>Los Datos Personales se ingresarán en Unit4 Student Management para permitir al Cliente organizar y administrar los procesos relacionados con el funcionamiento operativo y la gestión y / o procesos administrativos de su negocio interno. Los procesos pueden incluir:</p> <ul style="list-style-type: none"> • Reclutar futuros estudiantes, • Responder a solicitudes de información • Procesamiento de aplicaciones • Gestionar el ciclo de vida académico de un estudiante, incluida la incorporación, la programación de cursos, la progresión académica, el asesoramiento, la vivienda y otras instalaciones y/o la graduación. • Planificación y programación del personal docente <p>El procesamiento implicará:</p> <p>Producto (solución de software)</p> <p>Unit4 Student Management ejecutando código de software programable para que las actividades expuestas (arriba) puedan llevarse a cabo. Esto puede implicar la transferencia de datos hacia o desde soluciones de terceros que no están bajo el control del Encargado a través de integraciones.</p> <p>Servicios</p> <p>Transferencia y almacenamiento de Datos Personales para proporcionar Servicios adicionales como se establece con más detalle en la Descripción del Servicio o en la Descripción del Servicio de la Plataforma de Personas correspondiente.</p> <p>Acceso a los Datos Personales para proporcionar soporte y mantenimiento del Producto Unit4 y ayudar al cliente en el funcionamiento de la solución como se establece con más detalle en los Términos de Soporte de Unit4.</p> <p>Acceso a los Datos personales para proporcionar configuración y / o personalización y / o migración de datos (por ejemplo, de sus sistemas heredados) y / u otros Servicios profesionales comprados por el Cliente.</p>
Unit4 FP&A	<p>Los Datos Personales se ingresarán en Unit4 FP&A para permitir al Cliente organizar y administrar los procesos relacionados con el funcionamiento operativo y la gestión y / o procesos administrativos de su negocio interno. Los procesos pueden incluir:</p> <ul style="list-style-type: none"> • Presupuesto; • Informes financieros y de otro tipo; • Distribución de informes; • Procesos de aprobación; • Planificación de personas / proyectos. <p>El procesamiento implicará:</p> <p>Producto (solución de software)</p> <p>Unit4 FP&A ejecuta código de software programable para garantizar que las actividades establecidas (arriba) puedan tener lugar. Esto puede implicar la transferencia de datos hacia o desde soluciones de terceros que no están bajo el control del Encargado a través de integraciones.</p> <p>Servicios</p> <p>Transferencia y almacenamiento de Datos Personales para proporcionar Servicios adicionales como se establece con más detalle en la Descripción del Servicio o en la Descripción del Servicio de la Plataforma de Personas correspondiente.</p> <p>Acceso a los Datos Personales para brindar soporte y mantenimiento del Producto Unit4 y ayudar al Cliente en el funcionamiento de la solución como se establece con más detalle en los Términos de Soporte de Unit4.</p> <p>Acceso a los Datos personales para proporcionar configuración y / o personalización y / o migración de datos (por ejemplo, de sus sistemas heredados) y / u otros Servicios profesionales adquiridos por el Cliente.</p>
Unit4 Talent Management	<p>Los Datos Personales se ingresarán en Unit4 Talent Management para permitir al Cliente organizar y administrar los procesos relacionados con el funcionamiento operativo y los procesos de gestión y / o administrativos de su negocio interno. Los procesos pueden incluir:</p> <ul style="list-style-type: none"> • Gestión del capital humano; • Gestión del desempeño de los empleados; • Habilitación del talento; • Evaluación de candidatos; • Aprendizaje; • Comentarios y elogios; y • Análisis e interacción de personas. <p>El procesamiento implicará:</p> <p>Producto (solución de software)</p> <p>Unit4 Talent Management ejecuta código de software programable para garantizar que las actividades establecidas (como se detalla anteriormente) puedan llevarse a cabo. Esto puede implicar la transferencia de datos hacia o desde soluciones de terceros que no están bajo el control del Encargado a través de integraciones.</p> <p>Servicios</p>

	<p>Transferencia y almacenamiento de datos personales para proporcionar Servicios adicionales, como se establece con más detalle en la Descripción del Servicio o en la Descripción del Servicio de la Plataforma de Personas correspondiente.</p> <p>Acceso a los Datos Personales para brindar soporte y mantenimiento del Producto y ayudar al cliente en el funcionamiento de la solución como se establece en más detalle en los Términos de Soporte de Unit4</p> <p>Acceso a los Datos personales para proporcionar configuración y / o personalización y / o migración de datos (por ejemplo, de sus sistemas heredados) y / u otros Servicios profesionales comprados por el Cliente.</p>
<p>Unit4 Assistance PSA Suite</p>	<p>Los Datos Personales se ingresarán en Unit4 Assistance PSA Suite para permitir al Cliente organizar y administrar procesos relacionados con el funcionamiento operativo y la gestión y / o procesos administrativos de su negocio interno. Los procesos pueden incluir:</p> <ul style="list-style-type: none"> • automatización de una organización de servicios profesionales, incluida la gestión de recursos humanos y financieros (HRM); • gestión del tiempo y proyectos diarios; • reserva de tiempo y gastos con recibos; • transición de oportunidades a proyectos, presupuesto y previsión de horas y planificación de proyectos y recursos; • seguimiento de tiempo y gastos y ejecución de facturación; • integración de proyectos en otras aplicaciones y • realizar la contabilidad ayudando a la integración de datos financieros en otras soluciones. <p>El procesamiento implicará:</p> <p>Producto (solución de software)</p> <p>Unit4 Assistance PSA Suite ejecuta código de software programable para que las actividades establecidas (como se detalla anteriormente) puedan llevarse a cabo. Esto puede implicar la transferencia de datos hacia o desde soluciones de terceros que no están bajo el control del Encargado a través de integraciones.</p> <p>Servicios</p> <p>Transferencia y almacenamiento de datos personales para proporcionar Servicios adicionales como se establece con más detalle en la descripción del servicio o en la descripción del servicio de servicios de plataforma de personas correspondiente.</p> <p>Acceso a los datos personales para proporcionar soporte y mantenimiento del producto Unit4 y ayudar al cliente en el funcionamiento de la solución como se establece con más detalle en los términos de soporte de Unit4.</p> <p>Acceso a los Datos personales para proporcionar configuración y / o personalización y / o migración de datos (por ejemplo, de sus sistemas heredados) y / u otros Servicios profesionales comprados por el Cliente.</p>
<p>Servicios de plataforma de personas ("PPS"), Servicios de Localización y Apps de Unit4</p>	<p>Los datos serán procesados por el PPS, Servicios de Localización y/o las Apps de Unit4 para permitir los propósitos declarados de los servicios como se establece en la Descripción del Servicio de PPS disponible en www.unit4.com/terms.</p> <p>Además, los datos personales se ingresarán en Wanda mediante el software de terceros de su elección (por ejemplo, Slack Integration u otras aplicaciones de Microsoft (incluido Microsoft Teams). Dependiendo del Producto o Servicio de Unit4 utilizado por el Cliente, Wanda puede ayudar a completar las tareas administrativas de los empleados del Cliente.</p> <p>Las tareas pueden incluir:</p> <ul style="list-style-type: none"> • Entradas de la hoja de horas • Entradas de gastos • Solicitudes de viaje • Consultas sobre recibos de pago • Entradas de ausencias • Consultas de saldo • Requisitos de compra. <p>El procesamiento implicará:</p> <p>Producto (solución de software)</p> <p>Wanda ejecutando código de software programable para garantizar que las actividades establecidas (arriba) puedan tener lugar. Esto puede implicar la transferencia de datos hacia o desde soluciones de terceros que no están bajo el control del Encargado a través de integraciones.</p> <p>Servicios</p> <p>Transferencia y almacenamiento de Datos Personales para proporcionar Servicios adicionales como se establece con más detalle en la Descripción del Servicio o en la Plataforma de Personas correspondiente.</p> <p>Acceso a los datos personales para proporcionar soporte y mantenimiento de Unit4 PPS, Servicios de Localización y/o Apps y ayudar al cliente en el funcionamiento de la solución como se establece con más detalle en los términos de soporte de Unit4.</p> <p>Acceso a los Datos personales para proporcionar configuración y / o personalización y / o migración de datos (por ejemplo, de sus sistemas heredados) y / u otros Servicios profesionales comprados por el Cliente.</p> <p>Acceso a datos personales para la mejora del producto a través del aprendizaje automático de IA o el análisis de datos.</p>
<p>Unit4 Property Management</p>	<p>Los Datos Personales se ingresarán en Unit4 Property Management para permitir al Cliente organizar y administrar procesos relacionados con el funcionamiento operativo y la gestión y / o procesos administrativos de su negocio interno. Los procesos pueden incluir:</p> <ul style="list-style-type: none"> • registro de solicitantes; • gestión de arrendamientos; • procesos de contratación de alquileres;

<ul style="list-style-type: none"> • procesos de gestión de inquilinos; • procesos de firma electrónica; • adeudos incluida la impresión de facturas; • procesos de pagos; • procesos de reclamaciones; • cambio de alquileres; <p>El procesamiento implicará:</p> <p>Producto (solución de software)</p> <p>Unit4 Property Management ejecuta código de software programable para que las actividades establecidas (como se detalla anteriormente) puedan llevarse a cabo. Esto puede implicar la transferencia de datos hacia o desde soluciones de terceros que no están bajo el control del Encargado a través de integraciones.</p> <p>Servicios</p> <p>Transferencia y almacenamiento de datos personales para proporcionar Servicios como se establece con más detalle en la descripción del servicio o en la descripción del servicio de servicios de plataforma de personas correspondiente.</p> <p>Acceso a los datos personales para proporcionar soporte y mantenimiento del producto Unit4 y ayudar al Cliente en el funcionamiento de la solución como se establece con más detalle en los términos de soporte de Unit4.</p> <p>Acceso a los Datos personales para proporcionar configuración y / o personalización y / o migración de datos (por ejemplo, de sus sistemas heredados) y / u otros Servicios profesionales adquiridos por el Cliente.</p>
--

3. DESCRIPCIÓN DEL TRATAMIENTO Y MEDIOS:

El Encargado procesará los Datos personales antes mencionados en relación con las siguientes actividades (las actividades a continuación se mencionan solo como ejemplo):

Tipo de procesamiento	Descripción	Medios y recursos
Unit4 SaaS (General)	El Encargado procesará los Datos personales en relación con las actividades descritas en el Acuerdo y, más específicamente, en las Descripciones de los Servicios de Unit4.	<p><u>Personal</u></p> <p>El equipo de operaciones de Unit4 Cloud tiene personal en países miembros de la UE (incluyendo pero no limitado a Polonia, Suecia, Noruega, Países Bajos, España y Portugal), Reino Unido, Estados Unidos, Canadá, Malasia y Singapur. Personal del Encargado opera los Servicios SaaS.</p> <p><u>Activos e infraestructura</u></p> <p>Unit4 utiliza servicios de infraestructura de alojamiento de terceros para proporcionar Unit4 SaaS y emplea otros sistemas de software para la operación y la gestión. Consulte la Sección 3.</p>
U4 Talent Management SaaS	El Encargado procesará los Datos Personales en relación con las actividades descritas en el Acuerdo y, más específicamente, la Descripción del Servicio.	<p><u>Personal</u></p> <p>El equipo de operaciones de Unit4 Talent Management Cloud Services tiene personal principalmente en Bélgica y algunos otros países del EEE. Este personal del encargado opera el servicio SaaS de Unit4 Talent Management.</p> <p><u>Activos e infraestructura</u></p> <p>Unit4 utiliza servicios de infraestructura de alojamiento de terceros para proporcionar el servicio SaaS de Unit4 Talent Management y emplea otros sistemas de software para la operación y la administración. Consulte la Sección 3.</p>
Servicios de Soporte	El Encargado procesará los Datos personales en relación con las actividades descritas en el Acuerdo y más específicamente en los Términos de soporte de Unit4.	<p><u>Personal</u></p> <p>El equipo de soporte de Unit4 tiene personal en países miembros de la UE (incluyendo pero no limitado a Polonia, Suecia, Noruega, Alemania, Irlanda, Países Bajos, España y Portugal), Reino Unido, Estados Unidos, Canadá (y otras ubicaciones que puedan ser precisas para dar soporte a necesidades de negocio de Unit4). Personal del Encargado opera los Servicios SaaS. Este personal del Encargado proporciona los Servicios de soporte de Unit4 (establecidos en los Términos de soporte de Unit4 en la Sección B del SLA).</p> <p><u>Activos e infraestructura</u></p> <p>Unit4 utiliza otros sistemas de software para el funcionamiento, la prestación y la gestión de estos servicios.</p>
Servicios profesionales y / o consultoría	El Encargado procesará los Datos personales en relación con las actividades descritas en el Acuerdo y, más específicamente, en cualquier documentación del Proyecto o declaraciones de trabajo más detalladas acordadas entre las Partes después del inicio del Proyecto.	<p><u>Personal</u></p> <p>El equipo de Servicios Profesionales de Unit4 tiene personal en todas las ubicaciones donde Unit4 tiene una entidad de grupo corporativo que incluye Reino Unido, Irlanda, Polonia, Portugal, Noruega, España, Francia, Alemania, Suecia, EE. UU., Canadá, Singapur / Malasia (y otras ubicaciones según sea necesario para apoyar las necesidades comerciales de Unit4). Este personal del encargado proporciona los servicios profesionales de Unit4.</p> <p><u>Activos e infraestructura</u></p>

		Unit4 utiliza otros sistemas de software para el funcionamiento, la prestación y la gestión de estos servicios.
Unit4 Servicios profesionales (si se subcontrata a un partner)	<p>El Encargado y sus sub encargados Procesarán los Datos Personales antes mencionados en relación con las actividades descritas en el Acuerdo y (si corresponde) la documentación contractual y de servicios de terceros proporcionada como parte del Acuerdo. Para obtener más detalles, consulte la Sección 3.</p> <p>El Encargado ejecutará un acuerdo por escrito con el (los) Sub encargado (s), que estará de acuerdo con la legislación y regulaciones pertinentes.</p> <p>Además, el Responsable ha otorgado permiso al Encargado para contratar a los Sub encargados correspondientes según se enumeran en la Sección 3 al celebrar el Acuerdo.</p>	Consulte la Sección 3 o el formulario de pedido correspondiente.
Productos y servicios de terceros	El Encargado y sus sub encargados Procesarán los Datos Personales antes mencionados en relación con las actividades descritas en el Acuerdo y la documentación contractual y de servicio del Proveedor Tercero proporcionada como parte del Acuerdo.	Consulte la Sección 3 o el Formulario de pedido correspondiente y cualquier disposición adicional proporcionada en anexos o apéndices adicionales a la Información de procesamiento de datos si así lo requiere el Proveedor externo o la Ley aplicable.
Servicios de plataforma de personas ("PPS"), Servicios de Localización y Apps de Unit4	Además de Unit4 SaaS, el PPS, los Servicios de Localización y/o las Apps de Unit4 procesarán (cuando corresponda) los Datos personales en relación con una declaración de privacidad tal como se presenta al usuario final, solicitando su consentimiento, donde se procesan dichos Datos personales.	<p><u>Personal</u></p> <p>El equipo de operaciones de Unit4 Cloud Services, que opera el PPS, los Servicios de Localización y/o las Apps de Unit4 tiene personal en países miembros de la UE (incluyendo pero no limitado a Polonia, Suecia, Noruega, Países Bajos, España y Portugal) Reino Unido, Estados Unidos, Canadá, Malasia y Singapur. Este personal del encargado opera Unit4 SaaS.</p> <p><u>Activos e infraestructura</u></p> <p>Unit4 utiliza sus propios servicios de infraestructura y de terceros (compartidos) para proporcionar los servicios de Unit4 People Platform, Servicios de Localización y/o las Apps. Esto incluye sistemas de terceros (es decir, aplicaciones de colaboración), sobre los cuales Unit4 no tiene control. El PPS, incluido Wanda, Servicios de Localización y/o las Apps hacen uso de una serie de productos y servicios de Microsoft, de la siguiente manera:</p> <ul style="list-style-type: none"> • Servicios cognitivos: <ul style="list-style-type: none"> ○ Servicio cognitivo LUIS: comprensión del lenguaje. ○ API de traductor de texto: traducción de texto ○ Servicio QnA Maker Cognitive: proporciona un servicio de preguntas y respuestas • Conectores del marco de bots: proporciona la conexión de Wanda a los canales sociales compatibles. • Administrador de tráfico: se utiliza para la recuperación ante desastres y la conmutación por error si la región principal no está en buen estado. • Aplicaciones web / trabajos web: aloja API web y procesos basados en web de larga ejecución. • Bus de servicio: proporciona comunicación interna en el ecosistema de Wanda. • Cuentas de almacenamiento: se utilizan para almacenar el estado de la conversación y la configuración del usuario • Cosmos DB: proporciona almacenamiento • Funciones: proporciona algoritmos para extensiones • Cuadrícula de eventos: proporciona comunicación • Gestión de API: para gestionar APIs • Planes de Servicio: Linux y planes de servicio dinámico para el Servicio • Cuentas de almacenamiento: usadas para almacenamiento • Bóveda de claves: almacena datos confidenciales que se utilizan para comunicarse con los servicios de Microsoft y para los servicios internos. • Caché de Redis: proporciona capacidades de almacenamiento en caché • Application Insights: monitoreo del sistema, incluye telemetría y registro • Servidor SQL: proporciona almacenamiento • Kubernetes: contenedor de código abierto <p>Puede encontrar más información y detalles relacionados con esos productos y servicios de Microsoft aquí: https://azure.microsoft.com/en-us/services/.</p> <p>Asimismo, junto con el PPS, Servicios de Localización y/o las Apps de Unit4 utilizan:</p> <p>Twilio- sendgrid: para enviar mensajes de correo</p>

4. PERÍODO DE RETENCIÓN

El Encargado conservará los Datos personales durante la vigencia del Acuerdo.

Después del período de retención acordado, el Encargado devolverá los Datos personales al Responsable, en un formato con capacidad de migración establecido por el Encargado o destruirá inmediatamente los Datos personales sin retener una copia, a la primera solicitud del Responsable.

5. INFORMACIÓN SOBRE EL PAÍS (O LUGAR) DE TRATAMIENTO DE DATOS PERSONALES

Producto – on premise	Los datos se almacenan en los servidores del Responsable en su lugar principal de negocios u oficina registrada, debiendo notificarse a Unit4.			
Producto - Unit4 SaaS	Unit4 Cloud opera en varios centros de datos, incluida una presencia mundial en Microsoft Azure. Unit4 desplegará al cliente en la ubicación más lógica dependiendo de dónde resida el cliente (como se establece en un formulario de pedido). Todos los datos del Cliente se almacenarán solo en la zona geopolítica seleccionada y no se moverán fuera de ella sin el consentimiento explícito del cliente.			
	MODELO EN LA NUBE	ZONA GEO-POLÍTICA	UBICACIÓN DEL CENTRO DE DATOS	INSTALACIÓN O ASOCIACIÓN
	SAAS CLOUD	EU	DUBLIN / AMSTERDAM	MICROSOFT AZURE
	SAAS CLOUD	USA	LOCACIONES MULTIMPLES	MICROSOFT AZURE
	SAAS CLOUD	CANADÁ	TORONTO / QUEBEC CITY	MICROSOFT AZURE
	SAAS CLOUD	REINO UNIDO	LONDRES / CARDIFF	MICROSOFT AZURE
	SAAS CLOUD	ASIA	SINGAPUR / HONG KONG	MICROSOFT AZURE
	SAAS CLOUD	AUSTRALIA	VICTORIA / NEW SOUTH WALES	MICROSOFT AZURE
	SAAS CLOUD	NORUEGA	OSLO / STAVANGER	MICROSOFT AZURE
	SAAS CLOUD	SUECIA (NÓRDICOS)	SÅTRA Y SOLLENTUNA	CONAPTO
Product – Talent Management SaaS	Talent Management SaaS opera en Microsoft Azure cubriendo las zonas geopolíticas de la UE y el Reino Unido, con la zona que corresponda de acuerdo con la localización del Cliente. Todos los datos del Cliente, excepto para compartirlos con los sub encargados seleccionados en la Sección 3, se almacenarán solo en la zona geopolítica seleccionada y no se moverán fuera de ella sin el consentimiento explícito del cliente.			
Unit4 Support – Soporte estándar y otros servicios de soporte estándar	Unit4 Support utiliza software de terceros (como Salesforce / ServiceNow) para registrar y procesar Casos. Estos casos son accesibles para cualquier empleado de Unit4 que tenga acceso a software de terceros, como ingenieros de soporte, ingenieros de nube, consultores de servicios profesionales y gestión de servicios. El acceso está controlado por la gestión interna y los procesos organizativos, para garantizar que los consultores o ingenieros no accedan a los Datos personales en ubicaciones que no deberían tener acceso a detalles particulares del Cliente.			
	Ubicación del cliente	Principalmente, el soporte proviene de (pero puede incluir otros países de la UE):		
	Reino Unido e Irlanda	Reino Unido, Irlanda, Portugal y Polonia.		
	Suecia, Noruega, Dinamarca, Finlandia e Islandia	Polonia, Portugal, Noruega y Suecia.		
	EE.UU. y Canadá	Polonia, Portugal, EE.UU. y Canadá.		
	Resto de Europa	Polonia, Portugal y Alemania.		
	APAC	Polonia, Portugal y Singapur / Malasia.		
Unit4 Soporte – Soporte 24/7	Utilizando una metodología de "seguir el sol", el soporte de casos de clientes las 24 horas del día, los 7 días de la semana, podría ocurrir en cualquiera de las ubicaciones de soporte mencionadas anteriormente. así como en Países Bajos, España y cualquier otra localización necesaria para dar soporte a las necesidades de negocio de Unit4.			
Unit4 Soporte – Solo soporte EU	Si se elige el soporte solo para la UE, los Casos solo se admiten dentro de las ubicaciones de la UE enumeradas anteriormente para soporte estándar (en horario laboral).			
Servicios de plataforma de personas ("PPS") (generalmente) incluidos IDS y Wanda (junto con cualquier servicio de apoyo), Servicios de Localización y/o Apps.	Los PPS son servicios en la nube que utilizan infraestructura compartida y servicios de terceros que pueden no proporcionar aislamiento de zona geopolítica. A continuación se muestra una descripción general del PPS y el país (o lugar) de procesamiento de datos personales que utiliza ese servicio.			
	Servicio	Zona geo-política	Donde el servicio procesa o almacena datos	Principalmente, el soporte proviene de:
	Wanda	Cualquiera	Predominantemente dentro de la UE, pero puede estar en cualquier lugar donde haya un data center de Azure (por ejemplo, EE.UU.)	Países de la EU incluyendo Irlanda, Polonia, España, Estados Unidos y otras localizaciones de soporte global cuando sea necesario
PPS, Servicios de Localización y/o Apps.	Depende de la Implementación de la nube	El Servicio se presta y los datos se almacenan en la zona geo-política seleccionada.	Como anteriormente para Unit4 SaaS	
Servicios profesionales de Unit4 y función de éxito del	Ámbito	Los servicios profesionales y el éxito del cliente se proporcionan desde:		
	Implementación y otros servicios de proyectos	En el Territorio o ubicación del Cliente del domicilio social / lugar principal de negocios (según corresponda) y / o Portugal, según lo acordado entre las Partes en la documentación del proyecto o en una declaración de trabajo (si corresponde).		

cliente de Unit4	Migración de datos	En el Territorio o ubicación del Cliente del domicilio social / lugar principal de negocios (según corresponda) y / o Portugal, según lo acordado entre las Partes en la documentación del proyecto o en una declaración de trabajo (si corresponde).
	Solución de problemas	En la ubicación del Servicio de soporte de Unit4 correspondiente y en Portugal.
	Éxito del cliente	En la ubicación del Servicio de soporte de Unit4 correspondiente y en Portugal.

6. DETALLES DE CONTACTO

Para preguntas o comentarios sobre esta Información de procesamiento de datos, la persona de contacto es

Responsable del tratamiento: por carta (dirigida al responsable global de privacidad de datos, copia al departamento jurídico corporativo) P.O. Box 5005, 3528 BJ Utrecht, Países Bajos o por correo electrónico a privacy@unit4.com o a la dirección de Unit4 para los avisos proporcionados en el Acuerdo.

Encargado: La dirección del Responsable para avisos indicada en el Acuerdo.

SECCIÓN 2 – MEDIDAS DE SEGURIDAD

Como se indica en el párrafo 6 de los Términos de procesamiento de datos, las medidas de seguridad técnicas y organizativas se enumeran en esta Sección y se complementan o modifican si es necesario. El Responsable considera que estas medidas son adecuadas para el procesamiento de datos personales.

Medidas de seguridad empresarial de Unit4 (resumen de operaciones comerciales internas)

Descripción de las medidas de seguridad técnicas y organizativas implementadas por el Encargado en su organización (en general):

Seguridad física:

- El control de acceso físico es administrado por las instalaciones de Unit4.
- Todas las oficinas cuentan con sistemas de seguridad para controlar el acceso a través de barreras, p. Ej. puertas de entrada, mostradores de recepción con personal, puertas cortafuego con alarma, sistemas de detección de intrusos y/u oficinas con cerradura.
- Unit4 opera los controles de acceso con la ayuda de conocimiento personal, como una contraseña o un código de acceso personal; o con la ayuda de dispositivos, como un pase de seguridad;
- Las salas de servidores en el sitio (cuando corresponda) tienen controles físicos adicionales.
- El acceso a áreas seguras o información confidencial está restringido para evitar el acceso no autorizado de visitantes / personal no autorizado (a través de oficinas con cerradura o gabinetes con cerradura) y políticas operativas de escritorio despejado cuando corresponda.
- Los visitantes de Unit4 son controlados en la recepción (ya sea por una recepcionista dedicada u otro miembro del personal).
- Se utilizan trituradoras u otro método de eliminación seguro adecuado para documentos sensibles.

Seguridad virtual e informática:

- El gerente de línea responsable se asegurará de que los empleados y contratistas devuelvan todos los activos de Unit4 en su poder al terminar su contrato de trabajo o contrato mercantil. Los registros de esta devolución de activos se mantienen en el sistema.
- Unit4 tiene como objetivo clasificar la información como pública, confidencial, propietaria o sensible. En consecuencia, la información estaría protegida de acuerdo con su clasificación.
- Los medios (incluidos los discos duros) se eliminan de forma segura cuando ya no se necesitan. Todo el material sensible (discos duros, disquetes, etc.) se elimina mediante un software de eliminación garantizado (no mediante reformato o eliminación) antes de su eliminación o destrucción física.
- Antimalware: utilizamos la última versión de las soluciones estándar de la industria para proporcionar protección antivirus y antimalware.

Además, Unit4 utiliza:

- control de derechos asignados;
- registros y controles de acceso al sistema;
- medidas de recuperación;
- la capacidad de garantizar la confidencialidad, integridad, disponibilidad y flexibilidad continuas de los sistemas y servicios de procesamiento; y
- sistemas y procesos que le permitan restaurar la disponibilidad y el acceso a los Datos Personales de manera oportuna en caso de un incidente físico o técnico.
- Se han elaborado planes de continuidad del negocio y recuperación ante desastres que incluyen consideraciones de seguridad de la información.

Políticas de seguridad y documentación:

- El Equipo de Liderazgo Global de Unit4 y / o sus respectivos equipos de gestión local supervisan los planes de seguridad y gestión de la información tanto globales como locales, incluidas las políticas de seguridad de la información que cumplen con los riesgos de seguridad de la información identificados y respaldan los objetivos comerciales.
- La seguridad y la gestión de la información se asignan globalmente al Gerente de Seguridad de la Información y al Encargado de Protección de Datos Globales, quienes administran los recursos para brindar cumplimiento estratégico y general con la política y el proceso de seguridad de la información.
- Unit4 ha implementado políticas de seguridad actualizadas y enmendadas periódicamente para cumplir con las buenas prácticas de la industria.
- Unit4 tiene una política de privacidad y un libro blanco sobre GDPR publicados en www.unit4.com/terms.
- Unit4 suscribe acuerdos de confidencialidad y no divulgación con Terceros cuando comparte información confidencial relacionada con su negocio.
- Unit4 garantiza que todos los empleados y contratistas suscriban cláusulas de confidencialidad estándar en sus contratos.
- Unit4 proporciona a todos los empleados formación en relación con: protección de datos; seguridad y sus principios comerciales básicos como se indicó anteriormente.

Elementos adicionales para Unit4 SaaS en Microsoft Azure (resumen)

Descripción de las medidas de seguridad técnicas y organizativas implementadas por el Encargado en relación con la prestación de los servicios SaaS de Unit4:

Protección de datos

Unit4 Cloud utiliza varios mecanismos para proteger los Datos Personales en la nube. A continuación, se muestra una descripción general completa de los controles aplicados.

Funciones, procesos y protocolos de seguridad a nivel de red

- Transmisión segura de datos a través de redes públicas: todo el tráfico está protegido mediante protocolos estándar de la industria como SSL / TLS y HTTPS.
- Seguridad del sistema: mecanismo de autorización y autenticación lógica implementado
- Cortafuegos: tecnología de cortafuegos de próxima generación para garantizar que se controle el tráfico entrante y saliente.

Funciones, procesos y protocolos de seguridad a nivel de base de datos

- Seguridad de los datos: mecanismo de autorización y autenticación lógica implementado.
- Seguridad de la base de datos: cada cliente tiene su propia base de datos segura, lo que significa que no se requiere particionar las bases de datos y que los datos del cliente no se mezclan. El resultado es que los datos de un cliente nunca se comparten inadvertidamente con otros.
- Las copias de seguridad de las bases de datos se cifran utilizando tecnología de cifrado de base de datos completa, como el cifrado transparente de base de datos.
- Los ficheros y datos no transaccionales estarán asegurados por encriptado simétrico estándar (AES).
- Unit4 usa Azure Key Vault para mantener el control de las claves que usan las aplicaciones y los servicios en la nube para cifrar datos.

Seguridad continuamente probada y en evolución

Para descubrir vulnerabilidades imprevistas y refinar nuestras capacidades de detección y respuesta, estamos continuamente investigando cómo podemos mejorar nuestra seguridad para defendernos de posibles infracciones. El equipo de operaciones de Unit4 Cloud supervisa de cerca y asegura las operaciones

de Unit4 en la nube (infraestructura de nube, servicios de nube, productos, dispositivos y recursos internos), probando la penetración y mejorando nuestra capacidad para proteger, detectar y recuperarnos de las amenazas cibernéticas.

Detección, mitigación y respuesta de amenazas

A medida que ha aumentado el número, la variedad y la gravedad de las amenazas cibernéticas, también lo ha hecho nuestra diligencia en la detección y respuesta de amenazas. Los sistemas de monitoreo centralizados brindan visibilidad continua y alertas oportunas. La aplicación frecuente de parches y actualizaciones de seguridad ayuda a proteger los sistemas de vulnerabilidades conocidas. Los sistemas de detección de intrusiones y malware están diseñados para detectar y mitigar los riesgos de ataques externos. En caso de actividad maliciosa, nuestro equipo de respuesta a incidentes sigue los procedimientos establecidos para la gestión, comunicación y recuperación de incidentes. El equipo utiliza las mejores prácticas de la industria para alertar tanto a los equipos internos como a los clientes. Finalmente, los informes de seguridad monitorean los patrones de acceso para ayudar a identificar y mitigar de manera proactiva las amenazas potenciales.

Segregación de datos

Los datos son la moneda de la economía digital y nos tomamos muy en serio la responsabilidad de proteger los datos de los clientes. Tanto las salvaguardias tecnológicas, como las comunicaciones cifradas y los procesos operativos, ayudan a mantener seguros los datos del cliente. En la nube, los datos de varios clientes pueden almacenarse en los mismos recursos de TI. Unit4 utiliza el aislamiento lógico para segregar los datos de cada cliente de los de los demás. Unit4 SaaS está diseñado para contrarrestar los riesgos inherentes a un entorno multiusuario. El almacenamiento y el procesamiento de datos está lógicamente separado entre los consumidores que tienen instancias de base de datos separadas para todos nuestros clientes.

Cifrado de datos

Unit4 proporciona, de forma estándar, acceso seguro a todos sus servicios mediante el cifrado de todos los datos en tránsito que viajan por redes públicas. Esto se hace utilizando solo protocolos seguros, como HTTPS sobre TLS, utilizando los últimos cifrados de seguridad. El mecanismo utilizado es un cifrado de base de datos completo y transparente: TDE. Los clientes de Microsoft Azure en la oferta de SaaS público obtienen el cifrado de datos en reposo de TDE como estándar.

Control de acceso

Los clientes que utilizan los productos Unit4 en la nube están completamente autorizados para realizar un control de acceso de front-end a su aplicación. Esto significa que la responsabilidad de crear nuevas cuentas, la cancelación de la cuenta y la revisión de la aplicación Unit4 es del cliente.

Unit4 conservará el acceso de back-end limitado a los datos del cliente (mediante conexión directa a la base de datos). El acceso de Unit4 a Datos Personales se limitará estrictamente a las actividades necesarias para instalar, implementar, mantener, reparar, solucionar problemas o actualizar la solución. Todo el acceso se registra y se limita a un pequeño grupo de ingenieros de nube y consultores de soporte. Los registros de acceso se guardan en la solución de supervisión centralizada durante 365 días. En caso de filtraciones de datos, Unit4 puede proporcionar el registro de acceso a pedido.

Notificación de filtración de datos.

Unit4 notificará al Cliente sin demora injustificada después de tener conocimiento de una violación de datos. El cliente debe asegurarse de que los contactos enumerados en el portal de soporte de Unit4 estén siempre actualizados, ya que se utilizarán para todas las comunicaciones.

Privacidad y seguridad de los datos en el diseño

La plataforma Unit4 Cloud se diseñó desde cero con la seguridad y la privacidad de los datos en mente. Unit4 mejora continuamente la seguridad de la solución, aplicando las lecciones aprendidas de las pruebas de penetración y auditorías anuales.

Unit4 y los operadores de los centros de datos poseen varias certificaciones de seguridad; para obtener más detalles, consulte la Descripción del servicio que corresponda.

Elementos adicionales para los servicios de la plataforma Unit4 People (resumen)

Descripción de las medidas de seguridad técnicas y organizativas implementadas por el Encargado en relación con la prestación de los Servicios de la Plataforma Unit4 People (solo Cloud):

Protección de datos

Unit4 People Platform utiliza varios mecanismos para proteger los Datos Personales en la nube. A continuación, se muestra una descripción general completa de los controles aplicados.

Funciones, procesos y protocolos de seguridad a nivel de red

- Transmisión segura de datos a través de redes públicas: todo el tráfico está protegido mediante protocolos estándar de la industria como SSL / TLS y HTTPS.

Autenticación

Todos los servicios siguen el principio de autenticación y privilegios mínimos hacia los servicios y sus API están protegidas mediante mecanismos estándar de la industria. OpenID Connect y el protocolo OAuth 2.0 subyacente se utilizan para realizar de forma segura la autenticación de usuarios y / o servicios de clientes con partes de confianza y se valida la identidad y el acceso mediante tokens basados en notificaciones.

HMAC (Autenticación de mensajes basada en hash) se utiliza como método alternativo para asegurar la comunicación entre servicios.

Funciones, procesos y protocolos de seguridad a nivel de base de datos.

- Los datos almacenados en cuentas de almacenamiento se cifran en reposo.
- Todas las cuentas de almacenamiento requieren una transferencia segura: todo el tráfico está protegido mediante protocolos estándar de la industria, como SSL / TLS y HTTPS.
- Todos los datos almacenados en Azure Cosmos DB están cifrados en reposo y en transporte.
- Todos los servidores Azure SQL están habilitados con el cifrado de datos transparente (TDE).
- Todos los servidores Azure SQL se ejecutan con la detección de amenazas y la auditoría habilitadas.
- Azure KeyVault se usa para proteger información confidencial particular, como las credenciales de la entidad de servicio.

Funciones, procesos y protocolos de seguridad a nivel de mensajería.

- Todos los datos almacenados por instancias de Azure Service Bus están cifrados en reposo.
- Todo el tráfico (en tránsito) en Azure Service Bus está protegido mediante protocolos estándar de la industria como SSL

Puede encontrar más detalles sobre la Política de seguridad y el Programa de seguridad en www.unit4.com/terms

Cifrado de datos

Los servicios de Unit4 People Platform brindan, como estándar, acceso seguro a todos sus servicios mediante el cifrado de todos los datos en tránsito que viajan por redes públicas. Esto se hace utilizando solo protocolos seguros, como HTTPS sobre TLS (1.2), utilizando los últimos cifrados de seguridad. Todos los datos almacenados están encriptados.

Notificación de filtración de datos.

Unit4 notificará al Cliente sin demora injustificada después de tener conocimiento de una violación de datos. El cliente debe asegurarse de que los contactos enumerados en el portal de soporte de Unit4 estén siempre actualizados, ya que se utilizarán para todas las comunicaciones.

Privacidad y seguridad de los datos por diseño

Los servicios de Unit4 People Platform se diseñaron desde cero teniendo en cuenta la seguridad y la privacidad de los datos. Unit4 mejora continuamente la seguridad de la solución, aplicando las lecciones aprendidas de las pruebas de penetración y auditorías anuales.

SECCIÓN 3 – SUB ENCARGADOS UNIT4

Servicio	Sub encargado (nombre de la empresa, ubicación, etc.)	Lugar de procesamiento	Tipo de servicio por Sub encargado / Módulo utilizado con
Unit4 Professional Services (si se subcontrata a partner)	Como se especifica en el Acuerdo.	Como se especifica en el Acuerdo.	Como se especifica en el formulario de pedido o se acuerda por escrito con el cliente.
Los productos y servicios de terceros solo se aplican cuando los compra el cliente	Como se especifica en el Acuerdo.	Según lo dispuesto en el Acuerdo o en cualquier otro anexo o anexo del Acuerdo relacionado con el procesamiento del Proveedor Tercero.	Software y // o Servicios de soporte y / o Servicios en la nube.
Unit4 SaaS	Microsoft Azure	Como se indicó anteriormente en la Sección 1, párrafo 5.	Proporcionar infraestructura y servicios en la nube
	Microsoft Dynamics	Como se indicó anteriormente en la Sección 1, párrafo 5.	Proporcionar servicios de software, en particular Microsoft Dynamics (incluida alguna infraestructura en la nube).
	Microsoft	Como se indicó anteriormente en la Sección 1, párrafo 5.	Proporcionar herramientas de software y Office
	Conapto	Como se indicó anteriormente en la Sección 1, párrafo 5.	Proporcionar infraestructura y servicios en la nube
	Twilio-Sendgrid	Estados Unidos (Política de Privacidad)	Envío de correo (EU SCCs – Ver sección 4)
Unit4 SaaS – Talent Management	Microsoft Azure	Dublin, Irlanda	Brindando solución - Suite
	LogDNA	Estados Unidos de América (Política de privacidad)	Brindando solución - Suite (EU SCCs – Ver sección 4)
	Mandrill	Estados Unidos de América (Política de privacidad)	Brindando solución - Suite (EU SCCs – Ver sección 4)
	Mixpanel	Estados Unidos de América (Política de privacidad)	Brindando solución - Suite (EU SCCs – Ver sección 4)
	Rustici Software	AWS US-East-1 (Política de privacidad)	Proporcionar una solución: aprender (solo SCORM) (EU SCCs – Ver sección 4)
	Sentry	Estados Unidos de América (Política de privacidad)	Proporcionar una solución: suite (EU SCCs – Ver sección 4)
	Slack	Estados Unidos de América (Política de privacidad)	Proporcionar una solución: realizar (EU SCCs – Ver sección 4)
	Wistia	Estados Unidos de América (Política de privacidad)	Proporcionar una solución: aprender (EU SCCs – Ver sección 4)
Servicios de plataforma de personas ("PPS") (generalmente), incluidos IDS y Wanda (junto con cualquier servicio de apoyo)	Microsoft Azure	Como se indicó anteriormente en la Sección 1, párrafo 5 y según lo dispuesto por Microsoft aquí: https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located	Proporcionar servicios de plataforma e infraestructura en la nube (como se establece anteriormente) en la Sección 1.
	Twilio-Sendgrid	Estados Unidos (Política de Privacidad)	Envío de correo (EU SCCs – Ver sección 4)

SECCIÓN 4 – CLÁUSULAS CONTRACTUALES ESTÁNDARES PARA LA UE

CLÁUSULAS CONTRACTUALES TIPO (“CCT”)

Responsable a Encargado

Unit4 tiene la condición de encargado/importador de datos.

El Cliente tiene la condición de responsable/exportador de datos.

Con respecto a la relación entre las partes, es de aplicación el Módulo Dos (transferencia del responsable al encargado) de estas CCT.

Estas CCT sólo serán de aplicación cuando haya una transferencia de datos por parte del responsable del tratamiento de los datos personales dentro del EEE a un encargado situado fuera del EEE, también conocido como tercer país, y siempre que no se aplique ninguna decisión de adecuación.

ANEXO

CLÁUSULAS CONTRACTUALES TIPO

SECCIÓN I

Cláusula 1

Finalidad y ámbito de aplicación

- a) La finalidad de estas cláusulas contractuales tipo es garantizar que se cumplan los requisitos que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [\(1\)](#) (Reglamento general de protección de datos), exige para la transferencia de datos personales a un tercer país.
- b) Las partes:
- i) la(s) persona(s) física(s) o jurídica(s), autoridad(es) pública(s), servicio(s) u organismo(s) (en lo sucesivo, «entidad» o «entidades») que va(n) a transferir los datos personales, enumerada(s) en el anexo I.A (cada una denominada en lo sucesivo «exportador de datos»), y
 - ii) la(s) entidad(es) en un tercer país que va(n) a recibir los datos personales del exportador de datos directamente o indirectamente por medio de otra entidad que también sea parte en el presente pliego de cláusulas, enumerada(s) en el anexo I.A (cada una denominada en lo sucesivo «importador de datos»),
- han pactado las presentes cláusulas contractuales tipo (en lo sucesivo, «pliego de cláusulas»).
- c) El presente pliego de cláusulas se aplica a la transferencia de datos personales especificada en el anexo I.B.
- d) El apéndice del presente pliego de cláusulas, que contiene los anexos que se citan en estas, forman parte del pliego.

Cláusula 2

Efecto e invariabilidad de las cláusulas

- a) El presente pliego de cláusulas establece garantías adecuadas, incluidos derechos exigibles de los interesados y acciones judiciales eficaces, de conformidad con el artículo 46, apartado 1, y el artículo 46, apartado 2, letra c), del Reglamento (UE) 2016/679 y, en relación con las transferencias de datos de responsables a encargados o de encargados a otros encargados, de conformidad con las cláusulas contractuales tipo a que se refiere el artículo 28, apartado 7, del Reglamento (UE) 2016/679 siempre que no se modifiquen, salvo para seleccionar el módulo o módulos adecuados o para añadir o actualizar información del apéndice. Esto no es óbice para que las partes incluyan en un contrato más amplio las cláusulas contractuales tipo que contiene el presente pliego, ni para que añadan otras cláusulas o garantías adicionales siempre que no contradigan, directa o indirectamente, al presente pliego de cláusulas ni perjudiquen los derechos o libertades fundamentales de los interesados.
- b) El presente pliego de cláusulas se entiende sin perjuicio de las obligaciones a las que esté sujeto el exportador de datos en virtud del Reglamento (UE) 2016/679.

Cláusula 3

Terceros beneficiarios

- a) Los interesados podrán invocar, como terceros beneficiarios, el presente pliego de cláusulas contra el exportador y/o el importador de datos y exigirles su cumplimiento, con las excepciones siguientes.
- i) Cláusulas 1, 2, 3, 6 y 7.
 - ii) Cláusula 8: [módulo uno] cláusula 8.5, letra e), y cláusula 8.9, letra b); [módulo dos] cláusula 8.1, letra b), y cláusula 8.9, letras a), c), d) y e); [módulo tres] cláusula 8.1, letras a), c) y d), y cláusula 8.9, letras a), c), d), e), f) y g); [módulo cuatro] cláusula 8.1, letra b), y cláusula 8.3, letra b).
 - iii) Cláusula 9: [módulo dos] cláusula 9, letras a), c), d) y e); [módulo tres] cláusula 9, letras a), c), d) y e).
 - iv) Cláusula 12: [módulo uno] cláusula 12, letras a) y d); [módulos dos y tres] cláusula 12, letras a), d) y f).
 - v) Cláusula 13.
 - vi) Cláusula 15.1, letras c), d) y e).
 - vii) Cláusula 16, letra e).
 - viii) Cláusula 18: [módulos uno, dos y tres] cláusula 18, letras a) y b); [módulo cuatro] cláusula 18.

b) Lo dispuesto en la letra a) se entiende sin perjuicio de los derechos que el Reglamento (UE) 2016/679 otorga a los interesados.

Cláusula 4

Interpretación

- a) Cuando en el presente pliego de cláusulas se utilizan términos definidos en el Reglamento (UE) 2016/679, se entiende que tienen el mismo significado que en dicho Reglamento.
- b) El presente pliego de cláusulas deberá leerse e interpretarse con arreglo a las disposiciones del Reglamento (UE) 2016/679.
- c) El presente pliego de cláusulas no se podrá interpretar de manera que entre en conflicto con los derechos y obligaciones establecidos en el Reglamento (UE) 2016/679.

Cláusula 5

Jerarquía

En caso de contradicción entre el presente pliego de cláusulas y las disposiciones de acuerdos conexos entre las partes que estuvieren en vigor en el momento en que se pactare o comenzare a aplicarse el presente pliego de cláusulas, prevalecerá el presente pliego de cláusulas.

Cláusula 6

Descripción de la transferencia o transferencias

Los datos de la transferencia o transferencias y, en particular, las categorías de datos personales que se transfieren y los fines para los que se transfieren se especifican en el anexo I.B.

Cláusula 7 (opcional)

Cláusula de incorporación

- a) Cualquier entidad que no sea parte en el presente pliego de cláusulas podrá, previo consentimiento de todas las partes, adherirse al presente pliego de cláusulas en cualquier momento, ya sea como exportador de datos o como importador de datos, cumplimentando el apéndice y firmando el anexo I.A.
- b) Una vez haya cumplimentado el apéndice y firmado el anexo I.A, la entidad que se adhiera se considerará parte en el presente pliego de cláusulas y tendrá los derechos y obligaciones de un exportador de datos o un importador de datos, según la categoría en la que se haya inscrito en el anexo I.A.
- c) La entidad que se adhiera no adquirirá derechos y obligaciones del presente pliego de cláusulas derivados del período anterior a la adhesión.

SECCIÓN II: OBLIGACIONES DE LAS PARTES

Cláusula 8

Garantías en materia de protección de datos

El exportador de datos garantiza que ha hecho esfuerzos razonables para determinar que el importador de datos puede, aplicando medidas técnicas y organizativas adecuadas, cumplir las obligaciones que le atribuye el presente pliego de cláusulas.

MÓDULO DOS: transferencia de responsable a encargado

8.1. Instrucciones

- a) El importador de datos solo tratará los datos personales siguiendo instrucciones documentadas del exportador de datos. El exportador de datos podrá dar dichas instrucciones durante todo el período de vigencia del contrato.
- b) El importador de datos informará inmediatamente al exportador de datos en caso de que no pueda seguir dichas instrucciones.

8.2. Limitación de la finalidad

El importador de datos tratará los datos personales únicamente para los fines específicos de la transferencia indicados en el anexo I.B, salvo cuando siga instrucciones adicionales del exportador de datos.

8.3. Transparencia

Previo solicitud, el exportador de datos pondrá gratuitamente a disposición del interesado una copia del presente pliego de cláusulas, incluido el apéndice cumplimentado por las partes. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como las medidas descritas en el anexo II y datos personales, el exportador de datos podrá expurgar el texto del apéndice del presente pliego de cláusulas antes de compartir una copia, pero deberá aportar un resumen significativo si, de no hacerlo, el interesado no pudiese comprender el tenor del apéndice o ejercer sus derechos. Previo solicitud, las partes comunicarán al interesado los motivos del expurgo, en la medida de lo posible sin revelar la información expurgada. La presente cláusula se entiende sin perjuicio de las obligaciones que los artículos 13 y 14 del Reglamento (UE) 2016/679 atribuyen al exportador de datos.

8.4. Exactitud

Si el importador de datos tiene conocimiento de que los datos personales que ha recibido son inexactos o han quedado obsoletos, informará de ello al exportador de datos sin dilación indebida. En este caso, el importador de datos colaborará con el exportador de datos para suprimir o rectificar los datos.

8.5. Duración del tratamiento y supresión o devolución de los datos

El tratamiento por parte del importador de datos solo se realizará durante el período especificado en el anexo I.B. Una vez se hayan prestado los servicios de tratamiento, el importador de datos suprimirá, a petición del exportador de datos, todos los datos personales tratados por cuenta del exportador de datos y acreditará al exportador de datos que lo ha hecho, o devolverá al exportador de datos todos los datos personales tratados en su nombre y suprimirá las copias existentes. Hasta que se destruyan o devuelvan los datos, el importador de datos seguirá garantizando el cumplimiento con el presente pliego de cláusulas. Si el Derecho del país aplicable al importador de datos prohíbe la devolución o la destrucción de los datos personales, el importador de datos se compromete a seguir garantizando el cumplimiento del presente pliego de cláusulas y solo tratará los datos en la medida y durante el tiempo que exija el Derecho del país. Lo

anterior se entiende sin perjuicio de la cláusula 14 y, en particular, de la obligación que esta impone al importador de datos de informar al exportador de datos durante todo el período de vigencia del contrato si tiene motivos para creer que está o ha estado sujeto a normativa o prácticas que no se ajustan a los requisitos de la cláusula 14, letra a).

8.6. Seguridad del tratamiento

- a) El importador de datos y, durante la transferencia, también el exportador de datos aplicarán medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos; en particular, la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados (en lo sucesivo, «violación de la seguridad de los datos personales»). A la hora de determinar un nivel adecuado de seguridad, las partes tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para los interesados. Las partes deberán considerar, en particular, el cifrado o la seudonimización, especialmente durante la transmisión, si de este modo se puede cumplir la finalidad del tratamiento. En caso de seudonimización, la información adicional necesaria para atribuir los datos personales a un interesado específico quedará, en la medida de lo posible, bajo el control exclusivo del exportador de datos. Al cumplir las obligaciones que le impone el presente párrafo, el importador de datos aplicará, al menos, las medidas técnicas y organizativas que figuran en el anexo II. El importador de datos llevará a cabo controles periódicos para garantizar que estas medidas sigan proporcionando un nivel de seguridad adecuado.
- b) El importador de datos solo concederá acceso a los datos personales a los miembros de su personal en la medida en que sea estrictamente necesario para la ejecución, la gestión y el seguimiento del contrato. Garantizará que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.
- c) En caso de violación de la seguridad de datos personales tratados por el importador de datos en virtud del presente pliego de cláusulas, el importador de datos adoptará medidas adecuadas para ponerle remedio y, en particular, medidas para mitigar los efectos negativos. El importador de datos también lo notificará al exportador de datos sin dilación indebida una vez tenga conocimiento de la violación de la seguridad. Dicha notificación incluirá los datos de un punto de contacto en el que pueda obtenerse más información, una descripción de la naturaleza de la violación (en la que figuren, cuando sea posible, las categorías y el número aproximado de interesados y registros de datos personales afectados), las consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad, especialmente, en su caso, medidas para mitigar sus posibles efectos negativos. Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.
- d) El importador de datos deberá colaborar con el exportador de datos y ayudarlo para que pueda cumplir las obligaciones que le atribuye el Reglamento (UE) 2016/679, especialmente en cuanto a la notificación a la autoridad de control competente y a los interesados afectados, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el importador de datos.

8.7. Datos sensibles

En la medida en que la transferencia incluya datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales (en lo sucesivo, «datos sensibles»), el importador de datos aplicará las restricciones específicas y/o las garantías adicionales descritas en el anexo I.B.

8.8. Transferencias ulteriores

El importador de datos solo comunicará los datos personales a un tercero siguiendo instrucciones documentadas del exportador de datos. Por otra parte, solo se podrán comunicar los datos a terceros situados fuera de la Unión Europea [\(4\)](#) (en el mismo país que el importador de datos o en otro tercer país; en lo sucesivo, «transferencia ulterior») si el tercero está vinculado por el presente pliego de cláusulas o consiente a someterse a este, con elección del módulo correspondiente, o si:

- i) la transferencia ulterior va dirigida a un país sobre el que haya recaído una decisión de adecuación, con arreglo al artículo 45 del Reglamento (UE) 2016/679, que abarque la transferencia ulterior;
- ii) el tercero aporta de otro modo garantías adecuadas, con arreglo a los artículos 46 o 47 del Reglamento (UE) 2016/679, respecto del tratamiento en cuestión;
- iii) si la transferencia ulterior es necesaria para la formulación, el ejercicio o la defensa de reclamaciones en el marco de procedimientos administrativos, reglamentarios o judiciales específicos; o
- iv) si la transferencia ulterior es necesaria para proteger intereses vitales del interesado o de otra persona física.

La validez de las transferencias ulteriores depende de que el importador de datos aporte las demás garantías previstas en el presente pliego de cláusulas y, en particular, la limitación de la finalidad.

8.9. Documentación y cumplimiento

- a) El importador de datos resolverá con presteza y de forma adecuada las consultas del exportador de datos relacionadas con el tratamiento con arreglo al presente pliego de cláusulas.
- b) Las partes deberán poder demostrar el cumplimiento del presente pliego de cláusulas. En particular, el importador de datos conservará suficiente documentación de las actividades de tratamiento que se realicen por cuenta del exportador de datos.
- c) El importador de datos pondrá a disposición del exportador de datos toda la información necesaria para demostrar el cumplimiento de las obligaciones contempladas en el presente pliego de cláusulas y, a instancia del exportador de datos, permitirá y contribuirá a la realización de auditorías de las actividades de tratamiento cubiertas por el presente pliego de cláusulas, a intervalos razonables o si existen indicios de incumplimiento. Al decidir si se realiza un examen o una auditoría, el exportador de datos podrá tener en cuenta las certificaciones pertinentes que obren en poder del importador de datos.
- d) El exportador de datos podrá optar por realizar la auditoría por sí mismo o autorizar a un auditor independiente. Las auditorías podrán consistir en inspecciones de los locales o instalaciones físicas del importador de datos y, cuando proceda, realizarse con un preaviso razonable.
- e) Las partes pondrán a disposición de la autoridad de control competente, a instancia de esta, la información a que se refieren las letras b) y c) y, en particular, los resultados de las auditorías.

Cláusula 9

Recurso a subencargados

MÓDULO DOS: transferencia de responsable a encargado

- a)AUTORIZACIÓN GENERAL POR ESCRITO: El importador de datos cuenta con una autorización general del exportador de datos para contratar a subencargados que figuren en una lista acordada. El importador de datos informará al exportador de datos específicamente y por escrito de las adiciones o sustituciones de subencargados previstas en dicha lista con al menos [especificar período de tiempo] de antelación, de modo que el exportador de datos tenga tiempo suficiente para formular objeción a tales cambios antes de que se contrate al subencargado o subencargados de que se trate. El importador de datos proporcionará al exportador de datos la información necesaria para que este pueda ejercer su derecho a formular objeción.
- b)Cuando el importador de datos recurra a un subencargado para llevar a cabo actividades específicas de tratamiento (por cuenta del exportador de datos), lo hará por medio de un contrato escrito que establezca, en esencia, las mismas obligaciones en materia de protección de datos que las impuestas al importador de datos en virtud del presente pliego de cláusulas, especialmente en lo que se refiere a los derechos de los interesados en cuanto que terceros beneficiarios ⁽⁸⁾. Las Partes convienen que, al cumplir el presente pliego de cláusulas, el importador de datos también da cumplimiento a las obligaciones que le atribuye la cláusula 8.8. El importador de datos se asegurará de que el subencargado cumpla las obligaciones que le atribuya el presente pliego de cláusulas.
- c)El importador de datos proporcionará al exportador de datos, a instancia de este, una copia del contrato con el subencargado y de cualquier modificación posterior del mismo. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, el importador de datos podrá expurgar el texto del contrato antes de compartir la copia.
- d)El importador de datos seguirá siendo plenamente responsable ante el exportador de datos del cumplimiento de las obligaciones que imponga al subencargado su contrato con el importador de datos. El importador de datos notificará al exportador de datos los incumplimientos por parte del subencargado de las obligaciones que le atribuye dicho contrato.
- e)El importador de datos pactará con el subencargado una cláusula de tercero beneficiario en virtud de la cual, en caso de que el importador de datos desaparezca de facto, cese de existir jurídicamente o sea insolvente, el exportador de datos tendrá derecho a rescindir el contrato del subencargado y ordenar a este que suprima o devuelva los datos personales.

Cláusula 10

Derechos del interesado

MÓDULO DOS: transferencia de responsable a encargado

- a)El importador de datos notificará con presteza al exportador de datos las solicitudes que reciba del interesado. No responderá a dicha solicitud por sí mismo, a menos que el exportador de datos le haya autorizado a hacerlo.
- b)El importador de datos ayudará al exportador de datos a cumplir sus obligaciones al responder a las solicitudes de ejercicio de derechos que el Reglamento (UE) 2016/679 atribuye a los interesados. A este respecto, las partes establecerán en el anexo II medidas técnicas y organizativas apropiadas, teniendo en cuenta la naturaleza del tratamiento, por las que se garantice que se prestará ayuda al responsable a aplicar la presente cláusula, así como el objeto y el alcance de la ayuda requerida.
- c)En el cumplimiento de las obligaciones que le atribuyen las letras a) y b), el importador de datos seguirá las instrucciones del exportador de datos.

Cláusula 11

Reparación

- a)El importador de datos informará a los interesados, de forma transparente y en un formato de fácil acceso, mediante notificación individual o en su página web, del punto de contacto autorizado para tramitar reclamaciones. Este tramitará con presteza las reclamaciones que reciba de los interesados.
- [OPCIÓN: El importador de datos se aviene a que los interesados también puedan presentar una reclamación ante un organismo independiente de resolución de litigios ⁽¹¹⁾ sin coste alguno para el interesado. Informará a los interesados, en la forma establecida en la letra a), de este mecanismo de reparación y de que no están obligados a recurrir a este ni a seguir una secuencia concreta de vías de reparación.]
- b)En caso de litigio entre un interesado y una de las partes en relación con el cumplimiento del presente pliego de cláusulas, dicha parte hará todo lo posible para resolver amistosamente el problema de forma oportuna. Las partes se mantendrán mutuamente informadas de tales litigios y, cuando proceda, colaborarán para resolverlos.
- c)El importador de datos se compromete a aceptar, cuando el interesado invoque un derecho de tercero beneficiario con arreglo a la cláusula 3, la decisión del interesado de:
- presentar una reclamación ante la autoridad de control del Estado miembro de su residencia habitual o su lugar de trabajo o ante la autoridad de control competente con arreglo a la cláusula 13;
 - ejercitar una acción judicial en el sentido de la cláusula 18.
- d)Las partes aceptan que el interesado pueda estar representado por una entidad, organización o asociación sin ánimo de lucro en las condiciones establecidas en el artículo 80, apartado 1, del Reglamento (UE) 2016/679.
- e)El importador de datos acepta acatar las resoluciones que sean vinculantes con arreglo al Derecho aplicable de la UE o del Estado miembro de que se trate.
- f)El importador de datos acepta que la elección del interesado no menoscabe sus derechos sustantivos y procesales a obtener reparación de conformidad con el Derecho aplicable.

Cláusula 12

Responsabilidad

MÓDULO DOS: transferencia de responsable a encargado

- a)Cada parte será responsable ante la(s) otra(s) de cualquier daño y perjuicio que le(s) cause por cualquier vulneración del presente pliego de cláusulas.

- b) El importador de datos será responsable ante el interesado; el interesado tendrá derecho a que se le indemnice por los daños y perjuicios materiales o inmateriales que el importador de datos o su subencargado ocasionen al interesado por vulnerar los derechos de terceros beneficiarios que deriven del presente pliego de cláusulas.
- c) A pesar de lo dispuesto en la letra b), el exportador de datos será responsable ante el interesado; el interesado tendrá derecho a que se le indemnice por los daños y perjuicios materiales o inmateriales que el exportador de datos o el importador de datos (o su subencargado) ocasionen al interesado por vulnerar los derechos de terceros beneficiarios que deriven del presente pliego de cláusulas. Lo anterior se entiende sin perjuicio de la responsabilidad del exportador de datos y, cuando el exportador de datos sea un encargado que actúe por cuenta de un responsable, de la responsabilidad del responsable con arreglo al Reglamento (UE) 2016/679 o el Reglamento (UE) 2018/1725, según cuál sea de aplicación.
- d) Las partes acuerdan que, si el exportador de datos es considerado responsable, de conformidad con la letra c), de los daños o perjuicios causados por el importador de datos (o su subencargado), estará legitimado para exigir al importador de datos la parte de la indemnización que sea responsabilidad del importador de los datos.
- e) Cuando más de una parte sea responsable de un daño o perjuicio ocasionado al interesado como consecuencia de una vulneración del presente pliego de cláusulas, todas las partes responsables serán responsables solidariamente.
- f) Las partes acuerdan que, si una parte es considerada responsable con arreglo a la letra e), estará legitimada para exigir a la otra parte la parte de la indemnización correspondiente a su responsabilidad por el daño o perjuicio.
- g) El importador de datos no puede alegar la conducta de un subencargado del tratamiento para eludir su propia responsabilidad.

Cláusula 13

Supervisión

MÓDULO DOS: transferencia de responsable a encargado

- a) [Cuando el exportador de datos esté establecido en un Estado miembro de la UE:] La autoridad de control responsable de garantizar que el exportador de datos cumpla el Reglamento (UE) 2016/679 en cuanto a la transferencia de los datos, indicada en el anexo I.C, actuará como autoridad de control competente.

[Cuando exportador de datos no esté establecido en un Estado miembro de la UE, pero sí en un lugar que entre dentro del ámbito territorial de aplicación del Reglamento (UE) 2016/679, de conformidad con el artículo 3, apartado 2, y haya nombrado a un representante con arreglo al artículo 27, apartado 1, del Reglamento (UE) 2016/679:] La autoridad de control del Estado miembro en que esté establecido el representante en el sentido del artículo 27, apartado 1, del Reglamento (UE) 2016/679, indicada en el anexo I.C, actuará como autoridad de control competente.

[Cuando exportador de datos no esté establecido en un Estado miembro de la UE, pero sí en un lugar que entre dentro del ámbito territorial de aplicación del Reglamento (UE) 2016/679 de la Comisión, de conformidad con el artículo 3, apartado 2, y no haya nombrado a un representante con arreglo al artículo 27, apartado 2, del Reglamento (UE) 2016/679 de la Comisión:] La autoridad de control de uno de los Estados miembros en que estén situados los interesados cuyos datos personales se transfieran en virtud del presente pliego de cláusulas en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado, indicada en el anexo I.C, actuará como autoridad de control competente.

- b) El importador de datos da su consentimiento a someterse a la jurisdicción de la autoridad de control competente y a cooperar con ella en cualquier procedimiento destinado a garantizar el cumplimiento del presente pliego de cláusulas. En particular, el importador de datos se compromete a responder a consultas, someterse a auditorías y cumplir las medidas adoptadas por la autoridad de control y, en particular, las medidas correctivas e indemnizatorias. Remitirá a la autoridad de control confirmación por escrito de que se han tomado las medidas necesarias.

SECCIÓN III: DERECHO DEL PAÍS Y OBLIGACIONES EN CASO DE ACCESO POR PARTE DE LAS AUTORIDADES PÚBLICAS

Cláusula 14

Derecho y prácticas del país que afectan al cumplimiento de las cláusulas

MÓDULO DOS: transferencia de responsable a encargado

- a) Las partes aseguran que no tienen motivos para creer que el Derecho y las prácticas del tercer país de destino aplicables al tratamiento de los datos personales por el importador de datos, especialmente los requisitos para la comunicación de los datos personales o las medidas de autorización de acceso por parte de las autoridades públicas, impidan al importador de datos cumplir las obligaciones que le atribuye el presente pliego de cláusulas. Dicha aseveración se fundamenta en la premisa de que no se oponen al presente pliego de cláusulas el Derecho y las prácticas que respeten en lo esencial los derechos y libertades fundamentales y no excedan de lo que es necesario y proporcionado en una sociedad democrática para salvaguardar uno de los objetivos enumerados en el artículo 23, apartado 1, del Reglamento (UE) 2016/679.
- b) Las partes declaran que, al aportar la garantía a que se refiere la letra a), han tenido debidamente en cuenta, en particular, los aspectos siguientes:
- las circunstancias específicas de la transferencia, como la longitud de la cadena de tratamiento, el número de agentes implicados y los canales de transmisión utilizados; las transferencias ulteriores previstas; el tipo de destinatario; la finalidad del tratamiento; las categorías y el formato de los datos personales transferidos; el sector económico en el que tiene lugar la transferencia; el lugar de almacenamiento de los datos transferidos;
 - el Derecho y las prácticas del tercer país de destino —especialmente las que exijan comunicar datos a las autoridades públicas o autorizar el acceso de dichas autoridades— que sean pertinentes dadas las circunstancias específicas de la transferencia, así como las limitaciones y garantías aplicables ⁽¹²⁾;
 - las garantías contractuales, técnicas u organizativas pertinentes aportadas para complementar las garantías previstas en el presente pliego de cláusulas, especialmente incluidas las medidas aplicadas durante la transferencia y el tratamiento de los datos personales en el país de destino.
- c) El importador de datos asegura que, al llevar a cabo la valoración a que se refiere la letra b), ha hecho todo lo posible por proporcionar al exportador de datos la información pertinente y se compromete a seguir colaborando con el exportador de datos para garantizar el cumplimiento del presente pliego de cláusulas.
- d) Las partes acuerdan documentar la evaluación a que se refiere la letra b) y ponerla a disposición de la autoridad de control competente previa solicitud.
- e) El importador de datos se compromete a notificar al exportador de datos si, tras haberse vinculado por el presente pliego de cláusulas y durante el período de vigencia del contrato, tiene motivos para creer que está o ha estado sujeto a normativa o prácticas que no se ajustan a los requisitos de la letra

a), incluso a raíz de un cambio de la normativa en el tercer país o de una medida (como una solicitud de comunicación) que indique una aplicación de dicha normativa en la práctica que no se ajuste a los requisitos de la letra a). [Módulo tres: El exportador de datos notificará al responsable.]

f) De realizarse la notificación a que se refiere la letra e) o si el exportador de datos tiene motivos para creer que el importador de datos ya no puede cumplir las obligaciones que le atribuye el presente pliego de cláusulas, el exportador de datos determinará con presteza las medidas adecuadas (por ejemplo, medidas técnicas u organizativas para garantizar la seguridad y la confidencialidad) que deberán adoptar el exportador de datos y/o el importador de datos para poner remedio a la situación [módulo tres: si procede, tras consultar al responsable]. El exportador de datos suspenderá la transferencia de los datos si considera que no hay garantías adecuadas o si así lo dispone [módulo tres: el responsable o] la autoridad de control competente. En este supuesto, el exportador de datos estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas. Si el contrato tiene más de dos partes contratantes, el exportador de datos solo podrá ejercer este derecho de resolución con respecto a la parte pertinente, a menos que las partes hayan acordado otra cosa. En caso de resolución del contrato en virtud de la presente cláusula, será de aplicación la cláusula 16, letras d) y e).

Cláusula 15

Obligaciones del importador de datos en caso de acceso por parte de las autoridades públicas

MÓDULO DOS: transferencia de responsable a encargado

15.1. Notificación

a) El importador de datos se compromete a notificar con presteza al exportador de datos y, cuando sea posible, al interesado (de ser necesario, con la ayuda del exportador de datos) si:

i) recibe una solicitud jurídicamente vinculante de comunicación de datos personales transferidos con arreglo al presente pliego de cláusulas presentada por una autoridad pública (sobre todo, judicial) en virtud del Derecho del país de destino; dicha notificación contendrá información sobre los datos personales solicitados, la autoridad solicitante, la base jurídica de la solicitud y la respuesta dada; o

ii) tiene conocimiento de que las autoridades públicas han tenido acceso directo a los datos personales transferidos con arreglo al presente pliego de cláusulas en virtud del Derecho del país de destino; dicha notificación incluirá toda la información de que disponga el importador de datos.

[Módulo tres: El exportador de datos notificará al responsable.]

b) Si se prohíbe al importador de datos enviar la notificación al exportador de datos y/o al interesado en virtud del Derecho del país de destino, el importador de datos se compromete a hacer todo lo posible para obtener una dispensa de la prohibición, con el fin de comunicar toda la información disponible y lo antes posible. El importador de datos se compromete a documentar las actuaciones que realice a tal fin para poder justificar su diligencia si se lo pide el exportador de datos.

c) En la medida en que lo permita el Derecho del país de destino, el importador de datos se compromete a proporcionar al exportador de datos, a intervalos regulares durante el período de vigencia del contrato, la mayor cantidad posible de información pertinente sobre las solicitudes recibidas (en particular, el número de solicitudes, el tipo de datos solicitados, la autoridad o autoridades solicitantes, la impugnación de las solicitudes, el resultado de tales impugnaciones, etc.). [Módulo tres: El exportador de datos remitirá la información al responsable.]

d) El importador de datos se compromete a conservar la información a que se refieren las letras a) a c) durante el período de vigencia del contrato y a ponerla a disposición de la autoridad de control competente previa solicitud.

e) Las letras a) a c) se entenderán sin perjuicio de la obligación del importador de datos, contemplada en la cláusula 14, letra e), y en la cláusula 16, de informar con presteza al exportador de datos cuando no pueda dar cumplimiento al presente pliego de cláusulas.

15.2. Control de la legalidad y minimización de datos

a) El importador de datos se compromete a controlar la legalidad de la solicitud de comunicación y, en particular, si la autoridad pública solicitante está debidamente facultada para ello, así como a impugnar la solicitud si, tras una valoración minuciosa, llega a la conclusión de que existen motivos razonables para considerar que la solicitud es ilícita con arreglo al Derecho del país de destino, incluidas las obligaciones aplicables en virtud del Derecho internacional y los principios de cortesía internacional. El importador de datos agotará, en las mismas condiciones, las vías de recurso. Al impugnar una solicitud, el importador de datos instará la aplicación de medidas cautelares para suspender los efectos de la solicitud hasta que la autoridad judicial competente se haya pronunciado sobre el fondo. No comunicará los datos personales solicitados hasta que se lo exija la normativa procesal aplicable. Estos requisitos se entienden sin perjuicio de las obligaciones que la cláusula 14, letra e), atribuye al importador de datos.

b) El importador de datos se compromete a documentar sus valoraciones jurídicas y las impugnaciones de solicitudes de comunicación y a poner dicha documentación a disposición del exportador de datos en la medida en que lo permita el Derecho del país de destino. También pondrá dicha documentación a disposición de la autoridad de control competente previa solicitud. [Módulo tres: El exportador de datos pondrá la valoración a disposición del responsable.]

c) El importador de datos se compromete a proporcionar la mínima información posible al responder a las solicitudes de comunicación, basándose en una interpretación razonable de la solicitud.

SECCIÓN IV: DISPOSICIONES FINALES

Cláusula 16

Incumplimiento de las cláusulas y resolución del contrato

a) El importador de datos informará con presteza al exportador de datos en caso de que no pueda dar cumplimiento al presente pliego de cláusulas por cualquier motivo.

b) En caso de que el importador de datos incumpla las obligaciones que le atribuye el presente pliego de cláusulas, el exportador de datos suspenderá la transferencia de datos personales al importador de datos hasta que se vuelva a garantizar el cumplimiento o se resuelva el contrato. Lo anterior se entiende sin perjuicio de la cláusula 14, letra f).

c) El exportador de datos estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas cuando:

- i) el exportador de datos haya suspendido la transferencia de datos personales al importador de datos con arreglo a la letra b) y no se vuelva a dar cumplimiento al presente pliego de cláusulas en un plazo razonable y, en cualquier caso, en un plazo de un mes a contar desde la suspensión;
- ii) el importador de datos vulnere de manera sustancial o persistente el presente pliego de cláusulas; o
- iii) el importador de datos incumpla una resolución vinculante de un órgano jurisdiccional o autoridad de control competente en relación con las obligaciones que le atribuye el presente pliego de cláusulas.

En este supuesto, informará a la autoridad de supervisión competente [módulo tres: y al responsable] de su incumplimiento. Si el contrato tiene más de dos partes contratantes, el exportador de datos solo podrá ejercer este derecho de resolución con respecto a la parte pertinente, a menos que las partes hayan acordado otra cosa.

d) [Módulos uno, dos y tres: Los datos personales que se hayan transferido antes de la resolución del contrato con arreglo a la letra c) deberán, a elección del exportador de datos, devolverse inmediatamente al exportador de datos o destruirse en su totalidad. Lo mismo será de aplicación a las copias de los datos.] [Módulo cuatro: Los datos personales recopilados por el exportador de datos en la UE que se hayan transferido antes de la resolución del contrato con arreglo a la letra c) deberán destruirse en su totalidad inmediatamente, así como cualquier copia de estos.] El importador de datos acreditará la destrucción de los datos al exportador de datos. Hasta que se destruyan o devuelvan los datos, el importador de datos seguirá garantizando el cumplimiento con el presente pliego de cláusulas. Si el Derecho del país aplicable al importador de datos prohíbe la devolución o la destrucción de los datos personales transferidos, el importador de datos se compromete a seguir garantizando el cumplimiento del presente pliego de cláusulas y solo tratará los datos en la medida y durante el tiempo que exija el Derecho del país.

e) Ninguna de las partes podrá revocar su consentimiento a quedar vinculada por el presente pliego de cláusulas si: i) la Comisión Europea adopta una decisión de conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679 que regule la transferencia de datos personales a los que se aplique el presente pliego de cláusulas; o ii) el Reglamento (UE) 2016/679 pasa a formar parte del ordenamiento jurídico del país al que se transfieren los datos personales. Ello se entiende sin perjuicio de otras responsabilidades que sean de aplicación al tratamiento en cuestión en virtud del Reglamento (UE) 2016/679.

Cláusula 17

Derecho aplicable

MÓDULO DOS: transferencia de responsable a encargado

El presente pliego de cláusulas se regirá por el Derecho de uno de los Estados miembros de la Unión Europea, siempre que dicho Derecho admita la existencia de derechos de los terceros beneficiarios. Las partes acuerdan que sea el Derecho aplicable según el Contrato.

Cláusula 18

Elección del foro y jurisdicción

MÓDULO DOS: transferencia de responsable a encargado

- a) Cualquier controversia derivada del presente pliego de cláusulas será resuelta judicialmente en un Estado miembro de la Unión Europea.
- b) Las partes acuerdan que sean los órganos jurisdiccionales competentes en virtud del Derecho aplicable según el Contrato.
- c) Los interesados también podrán ejercer acciones judiciales contra el exportador de datos y/o el importador de datos en el Estado miembro en el que el interesado tenga su residencia habitual.
- d) Las partes acuerdan someterse a la jurisdicción de dicho Estado miembro.

⁽¹⁾ Cuando el exportador de datos sea un encargado del tratamiento sujeto al Reglamento (UE) 2016/679 que actúe por cuenta de una institución u organismo de la Unión como responsable del tratamiento, se considera que la utilización del presente pliego de cláusulas al recurrir a otro encargado (subtratamiento) no sujeto al Reglamento (UE) 2016/679 también garantiza el cumplimiento del artículo 29, apartado 4, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39), en la medida en que estén armonizados el presente pliego de cláusulas y las obligaciones en materia de protección de datos que imponga el contrato u otro acto jurídico celebrado entre el responsable y el encargado con arreglo al artículo 29, apartado 3, del Reglamento (UE) 2018/1725. Este será el caso, en particular, cuando el responsable y el encargado del tratamiento se basen en las cláusulas contractuales tipo incluidas en la Decisión 2021/915.

⁽²⁾ Para ello es necesario anonimizar los datos de tal manera que nadie pueda identificar a la persona, de conformidad con el considerando 26 del Reglamento (UE) 2016/679, y que este proceso sea irreversible.

⁽³⁾ El Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, el «Acuerdo EEE») dispone la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE (Islandia, Liechtenstein y Noruega). La legislación de la Unión sobre protección de datos y, en particular, el Reglamento (UE) 2016/679 están cubiertos por el Acuerdo EEE y han sido incorporados al anexo XI del mismo. Por lo tanto, toda comunicación del importador de datos a un tercero situado en el EEE no puede considerarse una transferencia ulterior a efectos del presente pliego de cláusulas.

⁽⁴⁾ El Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, el «Acuerdo EEE») dispone la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE (Islandia, Liechtenstein y Noruega). La legislación de la Unión sobre protección de datos y, en particular, el Reglamento (UE) 2016/679 están cubiertos por el Acuerdo EEE y han sido incorporados al anexo XI del mismo. Por lo tanto, toda comunicación del importador de datos a un tercero situado en el EEE no puede considerarse una transferencia ulterior a efectos del presente pliego de cláusulas.

⁽⁵⁾ Véase el artículo 28, apartado 4, del Reglamento (UE) 2016/679 y, cuando el responsable sea una institución u organismo de la UE, el artículo 29, apartado 4, del Reglamento (UE) 2018/1725.

⁽⁶⁾ El Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, el «Acuerdo EEE») dispone la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE (Islandia, Liechtenstein y Noruega). La legislación de la Unión sobre protección de datos y, en particular, el Reglamento (UE) 2016/679 están cubiertos por el Acuerdo EEE y han sido incorporados al anexo XI del mismo. Por lo tanto, toda comunicación del importador de datos a un tercero situado en el EEE no puede considerarse una transferencia ulterior a efectos del presente pliego de cláusulas.

(7) En concreto, si el tratamiento afecta a datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales.

(8) Este requisito podrá satisfacerse si el subencargado se adhiere al presente pliego de cláusulas, con elección del módulo correspondiente, con arreglo a la cláusula 7.

(9) Este requisito podrá satisfacerse si el subencargado se adhiere al presente pliego de cláusulas, con elección del módulo correspondiente, con arreglo a la cláusula 7.

(10) Dicho plazo podrá prorrogarse por un máximo de dos meses adicionales en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El importador de datos informará debidamente y con prontitud al interesado de cualquier prórroga de este tipo.

(11) El importador de datos solo podrá ofrecer una resolución independiente de los litigios a través de un órgano de arbitraje si está establecido en un país que haya ratificado el Convenio de Nueva York sobre la ejecución de laudos arbitrales.

(12) Por lo que se refiere al efecto de dicho Derecho y prácticas en el cumplimiento del presente pliego de cláusulas, a la hora de realizar una valoración integral de esta cuestión pueden tenerse en cuenta distintos aspectos. Uno de estos aspectos puede ser que haya experiencia práctica pertinente y documentada en casos anteriores de solicitudes de comunicación por parte de las autoridades públicas, o la ausencia de tales solicitudes, en un período suficientemente representativo. Con esto se quiere decir, en particular, los registros internos u otra documentación elaborados de forma continua con la diligencia debida y certificados en los niveles más altos de la dirección siempre que esta información pueda compartirse legalmente con terceros. Cuando se use esta experiencia práctica para llegar a la conclusión de que el importador de datos no tendrá impedimento para cumplir el presente pliego de cláusulas, deberá estar respaldada por otros elementos pertinentes y objetivos; corresponde a las partes valorar minuciosamente si la suma de estos factores es suficientemente determinante, en términos de fiabilidad y representatividad, para respaldar esta conclusión. En particular, las partes deben tener en cuenta si su experiencia práctica está corroborada y no se ve desmentida, por información que sea fiable y de dominio público o accesible de cualquier otro modo acerca de la existencia o ausencia de solicitudes en el mismo sector o acerca de la aplicación de la normativa de que se trate en la práctica, como jurisprudencia e informes de organismos de supervisión independientes.

APÉNDICE

NOTA ACLARATORIA:

Se debe poder distinguir claramente la información aplicable a cada transferencia o categoría de transferencias y, por tanto, determinar la función o funciones respectivas de las partes en cuanto exportador(as) de datos y/o importador(as) de datos. No es imprescindible cumplimentar y firmar apéndices separados por cada transferencia o categoría de transferencias y/o relación contractual si se puede lograr un nivel de transparencia equivalente cumplimentando un solo apéndice. No obstante, cuando sea necesario para garantizar claridad suficiente, deben utilizarse apéndices separados.

ANEXO I

A. LISTA DE PARTES

Exportador(es) de datos: *[Identidad y datos de contacto del exportador o exportadores de datos y, en su caso, del delegado de protección de datos de este o estos y/o del representante en la Unión Europea]*

Los que constan identificados en el Contrato.

Actividades relacionadas con los datos transferidos en virtud del presente pliego de cláusulas:

Las que constan descritas en el Contrato.

2. Rol (responsable/encargado):

Los que constan descritos en el Contrato.

Importador(es) de datos: *[Identidad y datos de contacto del importador o importadores de datos, incluyendo cualquier persona de contacto con responsabilidades sobre protección de datos]*

Los que constan identificados en el Contrato.

Actividades relacionadas con los datos transferidos en virtud del presente pliego de cláusulas:

Las que constan descritas en el Contrato.

B. DESCRIPCIÓN DE LA TRANSFERENCIA

Categorías de interesados cuyos datos personales se transfieren

Las que constan descritas en las Secciones 1 y 3 de la Información sobre el Tratamiento de Datos.

Categorías de datos personales transferidos

Las que constan descritas en las Secciones 1 y 3 de la Información sobre Tratamiento de Datos.

Datos sensibles transferidos (si procede) y restricciones o garantías aplicadas que tengan plenamente en cuenta la naturaleza de los datos y los riesgos que entrañan, como, por ejemplo, la limitación estricta de la finalidad, restricciones de acceso (incluido el acceso exclusivo del personal que haya hecho un curso especializado), un registro del acceso a los datos, restricciones a transferencias ulteriores o medidas de seguridad adicionales.

Las que constan descritas en las Secciones 1 y 3 de la Información sobre Tratamiento de Datos.

La frecuencia de la transferencia (por ejemplo, si los datos se transfieren de una vez o de forma periódica).

Las que constan descritas en las Secciones 1 y 3 de la Información sobre Tratamiento de Datos.

Naturaleza del tratamiento

Las que constan descritas en las Secciones 1 y 3 de la Información sobre Tratamiento de Datos.

Finalidad(es) de la transferencia y posterior tratamiento de los datos

Las que constan descritas en las Secciones 1 y 3 de la Información sobre Tratamiento de Datos.

El plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo

Las que constan descritas en las Secciones 1 y 3 de la Información sobre Tratamiento de Datos.

En caso de transferencia a (sub)encargados, especifíquese también el objeto, la naturaleza y la duración del tratamiento

Las que constan descritas en las Secciones 1 y 3 de la Información sobre Tratamiento de Datos.

C. AUTORIDAD DE CONTROL COMPETENTE

Indíquese la autoridad o autoridades de control competentes de conformidad con la cláusula 13

La autoridad de control competente será la autoridad de los Países Bajos:

“De Autoriteit Persoonsgegevens”.

(A menos que se requiera lo contrario en la cláusula 13).

ANEXO II

MEDIDAS TÉCNICAS Y ORGANIZATIVAS, EN ESPECIAL MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

NOTA ACLARATORIA:

Las medidas técnicas y organizativas deben describirse de manera concreta y no de manera genérica. Véase también el comentario general de la primera página del apéndice, especialmente en cuanto a la necesidad de indicar claramente qué medidas se aplican a cada transferencia o conjunto de transferencias.

Descripción de las medidas técnicas y organizativas aplicadas por los importadores de datos (inclusive las certificaciones pertinentes) para garantizar un nivel adecuado de seguridad, teniendo en cuenta la naturaleza, el alcance, el contexto y la finalidad del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas.

Aquellas descritas en la Sección 2 de la Información sobre el Tratamiento de Datos.

ANEXO III:

LISTA DE SUBENCARGADOS DEL TRATAMIENTO

NOTA ACLARATORIA:

Debe cumplimentarse este anexo respecto de los módulos dos y tres cuando sea necesaria la autorización específica de uno o más subencargados [cláusula 9, letra a), opción 1].

No aplicable.
