



Esta traducción se facilita a título informativo. Solo la versión alemana es jurídicamente vinculante. [Ver la versión alemana](#)

Contrato de encargo del tratamiento conforme al art. 28 del RGPD

Versión de 02.10.2026 (versión 1.0) · entre el cliente (titular de la cuenta de empresa) y secureIT UG (haftungsbeschränkt)

Nota: Este contrato se perfecciona con el registro de una cuenta de empresa en secureIT. No se requiere firma. Este documento sirve como justificante para su documentación y para su delegado de protección de datos.

Preámbulo

El cliente que encarga el tratamiento (la organización que crea una cuenta de empresa en secureIT, en adelante, el «Cliente») utiliza la plataforma secureIT de secureIT UG (haftungsbeschränkt), Weinstraße 9, 79282 Ballrechten-Dottingen, representada por su administrador Patrick Ihle (en adelante, el «Encargado»), para formaciones de concienciación y simulaciones de phishing dirigidas a sus empleados. En este contexto, el Encargado trata datos personales por cuenta del Cliente. El presente contrato regula los derechos y obligaciones de ambas partes conforme al art. 28 del RGPD. Se celebra con el registro de una cuenta de empresa y se aplica a todas las formaciones y simulaciones que se inicien a través de dicha cuenta.

§ 1 Objeto y duración

(1) El objeto es la puesta a disposición de la formación en línea, el envío de correos electrónicos de phishing simulados, el registro de las reacciones a los mismos, la elaboración de evaluaciones por equipos, certificados de participación y justificantes de formación, así como, de forma opcional, lecciones mensuales de repaso.

(2) El contrato tiene la misma duración que la cuenta de empresa. Finaliza con la eliminación de esta por parte del Cliente o con la terminación del acuerdo de uso.

§ 2 Naturaleza y finalidad del tratamiento, tipos de datos, interesados

(1) **Finalidad:** formación y concienciación de los empleados del Cliente en materia de phishing y seguridad de la información, y acreditación de dicha formación ante aseguradoras, clientes y autoridades de control.

(2) **Tipos de datos:** nombre, apellidos, dirección de correo electrónico profesional; enlace de acceso personal; progreso de aprendizaje (lecciones realizadas con fecha y hora, fecha de finalización, itinerario de aprendizaje, resultado de la prueba de conocimientos, preguntas formuladas sobre las lecciones); para cada correo electrónico simulado, la fecha y hora de envío, así como si se abrió, si se hizo clic en un enlace y si se introdujeron datos en la página de práctica; los datos técnicos generados en ese contexto (dirección IP, programa de correo electrónico, fecha y hora); número y fecha del certificado. Las contraseñas introducidas no se almacenan.

(3) **Interesados:** empleados y demás personas dadas de alta por el Cliente (por ejemplo, aprendices, personal eventual, colaboradores externos con buzón de correo profesional), así como los administradores del Cliente.

§ 3 Sujeción a instrucciones

(1) El Encargado trata los datos exclusivamente en el marco del presente contrato y conforme a las instrucciones documentadas del Cliente. El Cliente imparte las instrucciones a través de las funciones de la plataforma (dar de alta personas, iniciar la formación, detener la ronda de pruebas, eliminar personas) o en forma de texto a la dirección indicada en el aviso legal.

(2) Si el Encargado considera que una instrucción es contraria a derecho, lo comunicará sin demora al Cliente y podrá suspender su ejecución hasta que esta sea confirmada.

(3) El Encargado no utiliza los datos para fines propios, en particular no para publicidad, ni los comunica a terceros, salvo que el presente contrato disponga otra cosa.





§ 4 Confidencialidad y restricción del acceso

(1) El Encargado es una empresa unipersonal. Únicamente tiene acceso a los datos el administrador, que se ha comprometido a guardar confidencialidad y está sujeto al secreto de datos. Si en el futuro se recurre a empleados o contratistas, estos se comprometerán por escrito a guardar confidencialidad antes de acceder a los datos.

(2) El Encargado no pone a disposición del Cliente los resultados personales de la simulación de phishing (qué persona abrió, hizo clic o respondió a qué correo). El Cliente recibe exclusivamente evaluaciones anonimizadas por equipos, que requieren un tamaño mínimo de tres personas. El propio Encargado tiene acceso a los datos individuales con fines de mantenimiento y soporte; dicho acceso queda registrado.

§ 5 Medidas técnicas y organizativas

El Encargado adopta las medidas técnicas y organizativas descritas en el anexo conforme al art. 32 del RGPD y las desarrolla de forma continua. Las medidas podrán sustituirse por otras equivalentes, sin que el nivel de protección pueda disminuir por ello.

§ 6 Subencargados del tratamiento

(1) El Cliente autoriza la intervención de los siguientes subencargados del tratamiento:

- **IONOS SE**, Elgendorfer Str. 57, 56410 Montabaur, Alemania: alojamiento de la plataforma y de la base de datos, envío y recepción de correo electrónico. Tratamiento exclusivamente en centros de datos situados en Alemania.
- **ElevenLabs Inc.**, Nueva York, EE. UU.: síntesis de voz para determinadas plantillas de simulación con mensaje de voz. Solo se transmite el texto que se va a leer, que contiene como máximo el nombre de pila de la persona interesada. La base de la transferencia a un tercer país es el Marco de Privacidad de Datos UE-EE. UU. (EU-US Data Privacy Framework), siempre que el proveedor esté certificado en él; en caso contrario, las cláusulas contractuales tipo de la UE. Solo se recurre a este subencargado si el Cliente selecciona una plantilla de ese tipo.

(2) El Encargado informará al Cliente de cualquier cambio o incorporación de otros subencargados del tratamiento con al menos cuatro semanas de antelación, mediante correo electrónico a la dirección del administrador. El Cliente podrá oponerse dentro de dicho plazo por causa justificada; si no se alcanza un acuerdo, el Cliente podrá dar de baja la cuenta de empresa.

§ 7 Asistencia al Cliente

(1) El Encargado asiste al Cliente en la respuesta a las solicitudes de los interesados (acceso, rectificación, supresión, limitación, portabilidad de los datos). El Cliente puede efectuar directamente en la plataforma la supresión y rectificación de los datos de personas concretas.

(2) El Encargado asiste al Cliente en una evaluación de impacto relativa a la protección de datos y en las solicitudes de las autoridades de control, en la medida en que afecten al tratamiento derivado del presente contrato.

§ 8 Notificación de violaciones de la seguridad de los datos personales

El Encargado notificará al Cliente toda violación de la seguridad de los datos personales que afecte a datos del Cliente sin demora y, a más tardar, dentro de las 24 horas siguientes a tener conocimiento de ella, a la dirección del administrador. La notificación incluirá, en la medida en que se conozcan, la naturaleza y el alcance de la violación, las personas y datos afectados, las consecuencias probables y las medidas adoptadas. El plazo del Cliente conforme al art. 33 del RGPD (72 horas) no se ve afectado; el Encargado presta su apoyo en la notificación.

§ 9 Supresión y devolución

(1) Tras la finalización del contrato, el Encargado suprimirá todos los datos del Cliente en un plazo de 30 días, salvo que se oponga a ello una obligación legal de conservación (por ejemplo, datos de facturación conforme al § 147 AO (Código Tributario alemán) y al § 257 HGB (Código de Comercio alemán)). Previamente, el Cliente podrá descargar las evaluaciones por equipos y los justificantes de formación en formato PDF.

(2) Durante la vigencia del contrato, el Cliente puede eliminar en cualquier momento a personas concretas; la supresión abarca los datos de acceso, el progreso de aprendizaje y los resultados de simulación de dicha persona. Los certificados ya emitidos conservan su número de verificación, a fin de que los justificantes presentados sigan siendo verificables; el Cliente también





puede exigir su supresión.

(3) Las copias de seguridad se sobrescriben conforme a un ciclo fijo; de este modo, los datos suprimidos desaparecen también de las copias de seguridad, a más tardar, 30 días después de su supresión.

§ 10 Acreditaciones y controles

(1) El Encargado acredita el cumplimiento de sus obligaciones mediante el anexo al presente contrato, el registro de actividades de tratamiento y, previa solicitud, mediante una autodeclaración por escrito.

(2) El Cliente podrá, previo aviso con una antelación razonable (al menos 14 días) y dentro del horario comercial habitual, realizar controles o encargarlos a un auditor sujeto a obligación de confidencialidad, como máximo una vez por año natural, salvo que exista un motivo concreto. El esfuerzo del Encargado por controles que vayan más allá de la autodeclaración se remunerará en función del trabajo realizado.

§ 11 Responsabilidad del Cliente

El Cliente, como responsable del tratamiento, es competente para garantizar la licitud del tratamiento, en particular en lo relativo a la base jurídica frente a sus empleados (por regla general, el § 26, apdo. 1, de la BDSG (Ley Federal alemana de Protección de Datos) y el art. 6.1.f) del RGPD), la información a los empleados conforme al art. 13 del RGPD y, en caso de existir un comité de empresa, su participación conforme al § 87, apdo. 1, n.º 6, de la BetrVG (Ley alemana de Organización de las Empresas). A tal efecto, el Encargado pone a disposición una hoja informativa y un modelo de acuerdo de empresa, e incluye la información a los empleados en el correo electrónico de invitación.

§ 12 Responsabilidad y disposiciones finales

(1) La responsabilidad se rige por el art. 82 del RGPD y por las condiciones de uso.

(2) El Encargado comunicará al Cliente por correo electrónico las modificaciones del presente contrato; la versión vigente en cada momento puede consultarse en secureit.icu/auftragsverarbeitung. Se aplica el derecho alemán. Si alguna disposición fuera ineficaz, el resto del contrato seguirá siendo válido.

Anexo: Medidas técnicas y organizativas (art. 32 del RGPD)

Control de acceso físico y de acceso a los sistemas: funcionamiento en un centro de datos de IONOS en Alemania certificado según la norma ISO 27001. Acceso al servidor únicamente por SSH con clave a través de un puerto no estándar, bloqueo automático tras intentos fallidos repetidos. Acceso de administración a la plataforma únicamente con dirección de correo electrónico verificada y contraseña; las sesiones caducan.

Control de acceso a los datos: modelo de roles (superadministrador, administrador de empresa, socio que presta asistencia, docente, participantes). Los administradores de empresa solo ven su propia organización; no pueden consultar los resultados personales de las simulaciones. Los accesos de los socios que prestan asistencia se registran con nombre, fecha y hora.

Control de la comunicación y del transporte: todas las conexiones se realizan exclusivamente mediante TLS (HTTPS). Envío de correo electrónico a través del servidor de correo propio con SPF, DKIM y DMARC. No se transmiten datos de los participantes a terceros, salvo a los subencargados del tratamiento mencionados.

Control de introducción de datos: las acciones relevantes para la seguridad (inicio de formaciones, gestión de rondas de pruebas, supresiones, facturas, accesos de socios) se registran en un registro de auditoría con usuario, fecha y hora y dirección IP.

Minimización de datos: solo se recogen el nombre y la dirección de correo electrónico profesional. Las contraseñas introducidas en las páginas de práctica se descartan; solo se almacena el hecho de que se produjo una introducción de datos. La estadística del sitio web funciona sin cookies y sin perfiles de usuario.

Control de disponibilidad: copias de seguridad diarias de la base de datos, conservación conforme a un ciclo fijo, restaurabilidad comprobada; las actualizaciones de seguridad del servidor se instalan con prontitud.

Control de separación: los datos de los distintos clientes están separados lógicamente mediante identificadores de organización; cada consulta está limitada a la propia organización. Los sistemas de prueba y de producción están separados; los





secureIT

Daten und User schützen. Mit Sicherheit.

datos de prueba no se mezclan con datos reales.

Organización: registro de actividades de tratamiento conforme al art. 30 del RGPD; procedimiento documentado para incidentes de seguridad; revisión periódica de las medidas y de la plataforma en busca de vulnerabilidades; concepto de supresión conforme al § 9 del presente contrato.



secureIT

Daten und User schützen. Mit Sicherheit.