NOTIFICACIÓN DE BRECHA DE SEGURIDAD DE DATOS PERSONALES

(Art. 33 del Reglamento (UE) 2016/679 – RGPD y arts. 33 y 34 de la LOPDGDD)

A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD)

C/ Jorge Juan, 6 28001 – Madrid

D./Dña. Carlos Fernández Domínguez, mayor de edad, con DNI **71430882N**, actuando en nombre y representación de la entidad **ILUMINACIÓN FUTURA SOSTENIBLE S.L** con CIF **B24659401** y domicilio social en **Calle José María Suárez González, 10 bajo 24007 León** en su condición de **Responsable del Tratamiento**, comparece y, como mejor proceda en Derecho,

EXPONE

Que, en cumplimiento de lo dispuesto en el artículo 33 del Reglamento General de Protección de Datos (RGPD) y en los artículos 33 y 34 de la Ley Orgánica 3/2018 (LOPDGDD), procede a **notificar una brecha de seguridad** que afecta a datos personales tratados por esta entidad.

I. Identificación del incidente

Se ha producido un acceso no autorizado de una persona subcontratada por Full Circle, S.L con acceso al entorno ERP Odoo/Odoo.sh en producción y con credenciales del responsable del tratamiento (IFS). Mediante el uso indebido de credenciales con privilegios administrativos generadas de forma no autorizada entro dentro del propio sistema.

El incidente implicó la creación de un usuario con privilegios de administrador, la toma de control temporal del entorno, la eliminación de accesos legítimos y la imposibilidad de acceso al sistema por parte de los usuarios autorizados.

Asimismo, se ha constatado la descarga no autorizada de la base de datos completa del sistema el día 9 de abril de 2026 a las 15:58 GMT.

El sistema permaneció inaccesible desde la tarde del 9 de abril hasta el 10 de abril a las 20:30, momento en el que se recuperó el control, se reactivaron los usuarios y se verificó la estabilidad del entorno.

Posteriormente, mediante análisis forense, se ha confirmado que no se han producido alteraciones ni manipulaciones de los datos personales, si bien se ha verificado la existencia de una copia no autorizada de la base de datos.

Se ha identificado a la persona responsable del incidente, existiendo indicios de que su actuación estuvo motivada por un conflicto con el proveedor tecnológico, orientado a la interrupción del servicio, sin evidencia de uso indebido posterior de los datos en el momento de la notificación.

II. Naturaleza de los datos personales afectados

Los datos comprometidos incluyen:

- *Datos identificativos: nombre y apellidos, DNI.*
- *Datos de contacto: dirección postal, correo electrónico.*
- *Datos económicos y financieros.*
- *Datos de facturación y otra información administrativa vinculada a la relación comercial.*

No consta que los datos estuvieran cifrados en el momento del incidente.

III. Categorías y volumen de interesados afectados

El incidente afecta aproximadamente a **2.200 personas**, entre clientes, proveedores, usuarios internos y otros contactos comerciales.

IV. Circunstancias de la brecha y posible impacto

La brecha de seguridad podría suponer un **riesgo significativo** para los derechos y libertades de los interesados, pudiendo derivar en:

- *Suplantación de identidad.*
- *Fraude económico.*
- *Acceso indebido a información sensible.*
- *Uso malicioso de datos personales.*

Por tal motivo, se ha procedido a la **notificación a los afectados**, conforme al artículo 34 del RGPD.

V. Medidas adoptadas tras la detección

Una vez detectado el incidente, se adoptaron de forma inmediata las siguientes medidas técnicas y organizativas. Se ha procedido de forma inmediata tras la detección del incidente a la recuperación del control del sistema, eliminación de accesos no autorizados, restauración de usuarios legítimos, revisión de permisos y aseguramiento del entorno.

Se ha realizado un análisis forense completo que confirma la integridad de los datos personales.

Se han reforzado los controles de acceso, implantado medidas adicionales de seguridad, incluyendo autenticación reforzada, y revisado los procedimientos de gestión de usuarios.

VI. Comunicaciones:

1. **Notificación individualizada por correo electrónico** a los afectados el día 10 de abril de 2026.

2. **Comunicación del incidente a las Fuerzas y Cuerpos de Seguridad del Estado** (Policía). Nº de atestado: 6602/26
3. **Aviso al INCIBE** para su registro y asesoramiento.
4. **Cambio inmediato de todas las contraseñas** de acceso al sistema.
5. **Bloqueo de accesos sospechosos** y revisión de permisos.
6. **Comunicación formal al proveedor Odoo Cloud**, solicitando investigación y medidas correctoras.

VII. Proveedor de servicios implicado

El incidente afecta a la plataforma **Odoo ERP**, alojada en la infraestructura cloud del proveedor **Odoo Cloud**. **Encargado del tratamiento Full Circle S.L**, quien ha sido informado y se encuentra analizando el origen del acceso no autorizado.

VIII. Solicitud

Por todo lo expuesto,

SOLICITA

Que la **Agencia Española de Protección de Datos** tenga por presentada la presente **notificación de brecha de seguridad**, proceda a su registro y, en su caso, requiera la información adicional que estime necesaria, así como valore la apertura de actuaciones de investigación si lo considera oportuno.

En león, a 14 de abril de 2026

Fdo.: Carlos Fernández Domínguez

DNI: 71430882N