FORMACIÓN BÁSICA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Situación Actual

DOS LEGISLACIONES APLICABLES

1. Ley 15/2003, del 18 de diciembre, calificada de protección de datos personales (y los reglamentos que la desarrollan)

2. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril del 2016 relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de este datos y por la cual se deroga la Directiva 95/46/CE (REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS)

¿Dirijo mis productos y/o servicios a ciudadanos que se encuentran en la Unión Europea?

Conceptos básicos

¿Qué se considera un dato personal?

- Toda información sobre una persona física identificada o identificable (el interesado).
- Se considerará persona física identificable toda persona cuya identidad pueda identificarse, directa o indirectamente, en particular mediante un identificador, como, por ejemplo, un número, un número de identificación, datos de localización, un identificador en línea, o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural, o social de dicha persona.

¿Qué podemos considerar datos personales?

- Nombre y apellidos de clientes y/o trabajadores de ENSISA
- Número de teléfono de clientes y/o trabajadores de ENSISA
- Datos médicos de clientes y/o trabajadores de ENSISA
- Correo electrónico de clientes y/o trabajadores de ENSISA
- Imágenes de clientes y/o trabajadores de ENSISA.

- ¿Qué más se os ocurre?

Conceptos básicos

¿Qué son los datos personales sensibles o categorías especiales de datos?

- Son aquellos datos personales que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los datos genéticos, los datos biométricos cuando se usan para identificar de manera unívoca a una persona física, los datos relativos a la salud, o a la vida sexual, o la orientación sexual de una persona física.

Queda prohibido el tratamiento de dichos datos exceptuando cuando concurran una de las circunstancias legalmente previstas.

¿Qué podemos considerar datos sensibles?

- La eventual alergia de un cliente de ENSISA
- Información relativa a una secuela física de un cliente de ENSISA
- Datos relativos a la salud de un cliente que nos comunica durante alguna gestión administrativa

- ¿Qué más se os ocurre?

Conceptos básicos

¿Qué es un tratamiento de datos personales?

- Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, tales como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, confrontación, o interconexión, limitación, supresión o destrucción.

¿Qué se puede considerar un tratamiento?

- Acceder o consultar bases de datos de clientes y/o trabajadores que contengan datos personales.
- Consultar lo que hay en un teléfono móvil perdido en las pistas.
- Publicar una foto de una persona en un sitio web o red social.
- Tomar de fotografías de un accidente en pistas.
- ¿Qué más se os ocurre?

Ciclo de vida de un dato personal

Las obligaciones en materia de protección de datos personales no se limitan únicamente a la fase de recogida sino que también se aplican a todo el ciclo de vida del dato personal.

1. Precauciones en el momento de la recogida

1.1.- Principio de minimización de datos

Recoger, única y exclusivamente, los datos necesarios para la finalidad de que se trate.

1.2.- Principio de transparencia

Informar al interesado del tratamiento que se realizará en relación con sus datos personales recogidos.

La información siempre deberá facilitarse por escrito (Principio de Responsabilidad Proactiva).

1.3.- Principio de licitud del tratamiento

Toda recogida y tratamiento de datos personales debe tener una base legal para el tratamiento.

Ejemplo: el consentimiento del interesado.

2. Tratamiento y custodia

2.1.- El tratamiento debe realizarse:

- Conforme a la información facilitada al interesado (principio de lealtad del tratamiento);
- Únicamente para la finalidad para la que se ha recogido (principio de limitación de la finalidad);
- Sobre datos reales y exactos, y si fuera necesario actualizados (principio de exactitud);
- Únicamente durante el tiempo necesario para alcanzar la finalidad para la que se recogieron los datos (principio de limitación del plazo de conservación); y
- De tal manera que se garantice una seguridad adecuada de los datos personales, y, por tanto, se deberán establecer las medidas técnicas u organizativas apropiadas (principio de integridad y confidencialidad).

Siempre se deberá disponer de evidencias del cumplimiento de todo lo anterior (principio de responsabilidad proactiva).

3. Comunicaciones de datos

¿QUÉ ES LA COMUNICACIÓN DE DATOS?

- Cualquier acceso o transmisión de datos personales a favor de un tercero destinatario de los datos.

¿QUÉ ES UN DESTINATARIO DE DATOS?

- La persona física o jurídica, de naturaleza pública o privada, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.

¿QUÉ ES UN ENCARGADO DE TRATAMIENTO?

- La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta de la empresa. Por lo tanto, se considerará que los tratamiento que realice el encargado será como si los llevara a cabo la empresa.

¿QUIÉN PUEDE SER UN "TERCERO"?

- Un prestador de servicios informáticos (encargado de tratamiento),

- Un prestador de servicios de riesgos laborales (encargado de tratamiento),

- Autoridades a las que se dan datos de accidentes en pistas (destinatario por obligación legal),

¿Qué más se os ocurre?

4. Derechos de los interesados

Mientras ENSISA trate los datos personales de los interesados, éstos podrán ejercer, entre otros, los siguientes derechos:

- Derecho de acceso (principio de transparencia),
- Derecho de rectificación (principio de exactitud),
- Derecho de supresión (principio de limitación de conservación),
- Derecho de limitación del tratamiento,
- Derecho de oposición al tratamiento, y
- Derecho a la portabilidad de los datos.

Obligación de respuesta a un ejercicio de derechos de un interesado (principio de transparencia) y deber de poder demostrar dicha respuesta (principio de responsabilidad proactiva).

5. Finalización del tratamiento

- **Por expiración del plazo de conservación (principio de limitación del plazo de conservación); y**

- **Debido al ejercicio del derecho de supresión, oposición o limitación por parte del interesado.**

3. Buenas y malas prácticas

MALAS PRÁCTICAS

- Guardo toda la información que me llega (por si acaso)
- Me voy de mi lugar de trabajo y dejo la sesión abierta del ordenador.
- Tengo la contraseña de mi ordenador a la vista.
- Dejo a la vista las fichas de los clientes.
- Apunto datos personales en un post-it y lo pierdo.
- Uso los datos personales para finalidades incompatibles con las que me llevaron a recogerlos
- Utilizo dispositivos personales para guardar información de la empresa.
- Utilizo mi correo electrónico personal para comunicarse con clientes.
- Utilizo mi whatsapp personal para comunicarse con clientes.
- Utilizo mis redes sociales para subir fotos con los clientes.

BUENAS PRÁCTICAS

- Borrar la información de la que no soy responsable.
- Me voy de mi sitio y cierro la sesión del ordenador.
- Conservo la contraseña en un lugar seguro.
- Mantengo la información de los clientes que administro con la máxima diligencia y confidencialidad.
- Destruyo el post-it donde he apuntado datos personales.
- Uso los datos personales exclusivamente para lo que los recogí.
- Utilizo las herramientas que me facilita la empresa para almacenar la información.
- Utilizo las herramientas que me facilita la empresa para comunicar con clientes.
- No utilizo mis redes sociales para subir fotos con los clientes.

6. Obligaciones

- Los datos personales serán «tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental»
- La Empresa «tomará medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales sólo pueda tratar estos datos siguiendo sus instrucciones»

<u>Obligación legal y cláusulas del contrato laboral</u>

- El trabajador estará sujeto al deber de confidencialidad
- El deber de confidencialidad se mantiene incluso después de finalizar la relación laboral

El trabajador debe velar por la seguridad de los datos de carácter personal en el tratamiento que participe, y tiene el deber de actuar siguiendo las instrucciones de la empresa, que es la responsable de los datos.

Las conductas contrarias al «deber de protección de datos personales» pueden ser consideradas constitutivas de infracciones muy graves por las autoridades, justificativas del despido o, incluso, derivar en reclamaciones civil o penales.

5. Régimen sancionador

Régimen sancionador de Andorra:

- 1er incumplimiento: máximo de 50.000 Euros,
- Incumplimientos subsiguientes: máx. 100.000 Euros.

Régimen sancionador de la Unión Europea:

- Infracciones consideradas graves: máximo 10 millones Euros o 2% del volumen de negocio total anual global del ejercicio financiero anterior.
- Infracciones consideradas "más graves": máximo 20 millones Euros o 4% del volumen de negocio total anual global del ejercicio financiero anterior.
    - No atender un ejercicio de derecho en el plazo y forma debidas.
    - Tratamiento ilícito de datos personales.
    - Comunicar datos personales a un destinatario que se encuentre en un país que no disponga de un nivel adecuado de protección de datos personales.

¡MUCHAS GRACIAS POR SU ATENCIÓN!

Ahora solo te queda responder el test:

https://forms.gle/Ukmo28n4pzGrYojp8