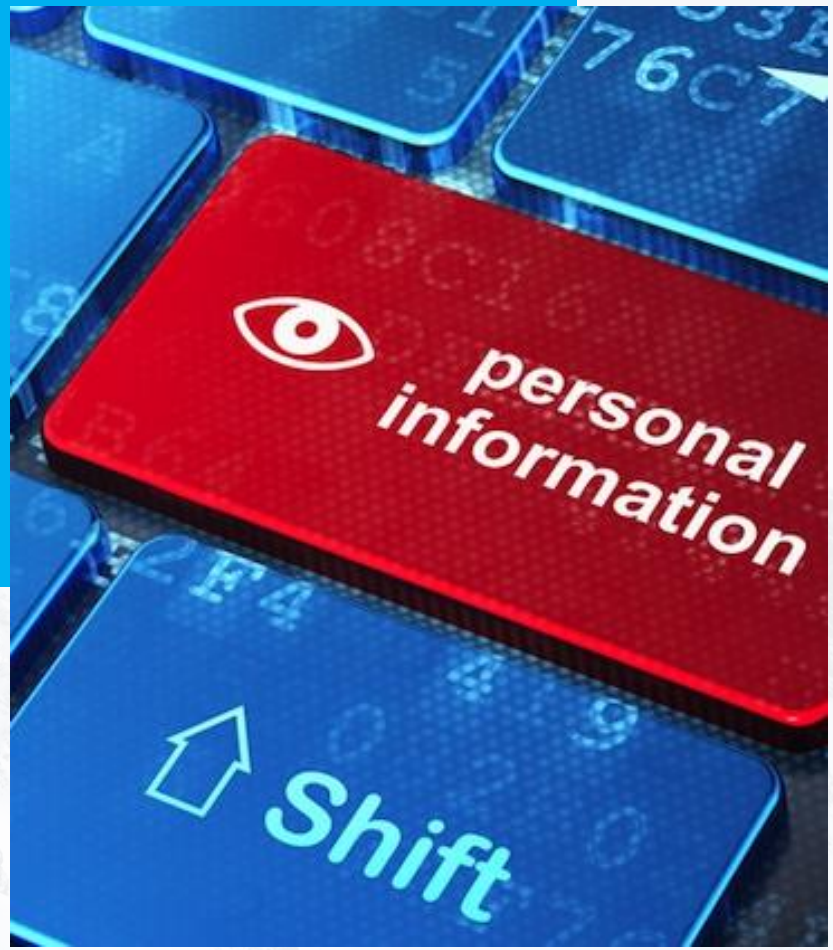
GRANDVALIRA
Grandvalira Resorts
ANDORRA

# FORMACIÓN BÁSICA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

## BUENAS PRÁCTICAS EN LA APLICACIÓN DEL RGPD Y LA LEY 29/2021, DEL 28 DE OCTUBRE, CUALIFICADA DE PROTECCIÓN DE DATOS PERSONALES (NUEVA LQPD) EN ENSISA

**Noviembre 2023**



# ¿QUÉ SE ENTIENDE POR "DATOS PERSONALES"?

Toda información sobre una persona física identificada o identificable (la persona interesada).

Por ejemplo: el nombre, el número de identificación, los datos de localización, un identificador en línea, uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural, o social de esta persona.

CATEGORÍAS ESPECIALES: que rebelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los datos genéticos o biométricos, datos relativos salud o vida sexual, o las orientaciones sexuales de una persona física.

QUEDA PROHIBIDO EL TRATAMIENTO DE ESTOS DATOS
EXCEPTUANDO CUANDO CONCURRAN ALGUNAS DE LAS CIRCUNSTANCIAS LEGALMENTE PREVISTAS.

# ¿QUÉ SE ENTIENDE POR “TRATAR"DATOS PERSONALES”?

Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, 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 interconexionado, limitación, supresión o destrucción.

Hojear, confirmar un dato, ...
todo el que tiene que ver con datos personales (por mínimo que sea)

# 02-OBLIGACIONES

- Los datos personales tienen que ser 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.

- ENSISA 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.

Obligación legal y cláusulas del contrato laboral:

- ✓ La persona trabajadora está sujeta al deber de confidencialidad.
- ✓ El deber de confidencialidad se mantiene incluso después de finalizar la relación laboral.

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

# 03-MALAS Y BUENAS PRÁCTICAS

## MALAS PRÁCTICAS

- Guardo toda la información que me llega (por si acaso).
- Me voy de mi puesto 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 la información para finalidades diferentes para la que se recogió.
- Utilizo dispositivos personales para guardar información de la empresa.
- Utilizo mi correo electrónico personal para comunicarme con clientes.
- Utilizo mi whatsapp personal para comunicarme con clientes.
- Utilizo mis redes sociales para subir fotos con los clientes.

# 03-MALAS Y BUENAS PRÁCTICAS

## BUENAS PRÁCTICAS

- Me voy de mi lugar y cierro la sesión del ordenador.
- Conservo la contraseña en un lugar que no sea accesible a nadie.
- Mantengo la información de los clientes que gestiono con la máxima diligencia y confidencialidad.
- Destruyo el post-it donde he apuntado datos personales.
- Uso la información exclusivamente para las finalidades para las cuales se recogieron.
- Utilizo las herramientas que me facilita la empresa para comunicarme con clientes.
- No utilizo mis redes sociales para subir fotos con los clientes.

# 03-MALAS Y BUENAS PRÁCTICAS

## RIESGOS

- Pantalla sin bloquear
- Juicejacking (cargador falso)
- Vulnerabilidades de las Apps
- SMS y enlaces nocivos
- Malware, etc.
- Acceso remoto no autorizado
- Geolocalización
- Pérdida o robo
- Eliminación accidental
- Acceso inalámbrico no autorizado
- Mensajes nocivos
- Apps que piden permiso para acceder a todo

La principal brecha de seguridad reportada por las empresas este año fue la pérdida de dispositivos (móviles, portátiles, USB, etc.), seguida del robo de los mismos.

# 03-MALAS Y BUENAS PRÁCTICAS

## BUENAS PRÁCTICAS

- Seguridad de las contraseñas
- Pantalla de bloqueo y limitar accesos rápidos desde dicha pantalla
- No dejar el dispositivo desatendido y desbloqueado
- No usar cargadores de la calle
- Actualizaciones automáticas
- Prudència con los enlaces sospechosos
- Cifrar el contenido (ficheros de los pendrives, memória interna del dispositivo y tarjetas SD)
- Hacer copias de seguridad
- Deshabilitar el NFC y el Bluetooth cuando no se utilicen
- Limitar la geolocalización
- No usar Wi-Fis públicas
- Pedir permiso para instalar nuevo software o nuevas Apps
- No permitir que una App examine los contactos

# RÉGIMEN SANCIONADOR

¡ATENCIÓN!

Régimen sancionador de la Unión Europea:

- Infracciones consideradas leves: máximo 10.000.000€ o 2% del volumen de negocio total anual global del ejercicio financiero anterior.
- Infracciones consideradas graves: máximo 20.000.000€ o 4% del volumen de negocio total anual global del ejercicio financiero anterior.

Régimen sancionador de Andorra:

- Infracciones consideradas muy graves: se sancionan con un importe comprendido entre 30.001€ y 100.000€.
- Infracciones consideradas graves: se sancionan con un importe comprendido entre 15.001€ y 30.000€.
- Infracciones consideradas leves: se sancionan con un importe comprendido entre 500€ y 15.000€.

GRANDVALIRA
Grandvalira Resorts
ANDORRA

# QUIZ FORMACIÓN BÁSICA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Quizizz

Playing a Game - Quizizz