Formación Interna

Protección de datos personales

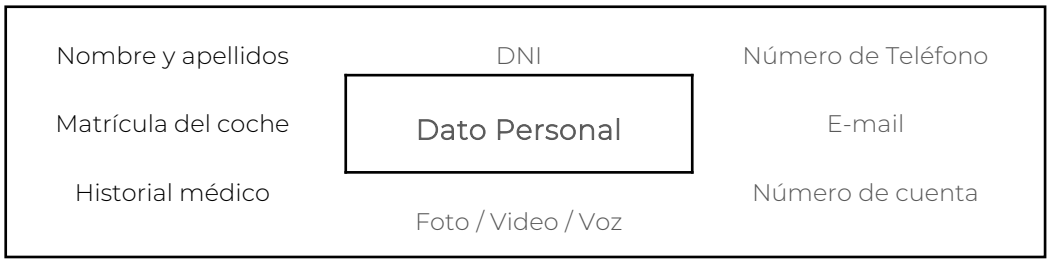
Contenido

- Introducción
- La Protección de datos en nuestro día a día
- Buenas prácticas

Introducción

¿Qué son los datos personales?

Los datos personales son toda aquella información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, 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.



¿Por qué hay que protegerlos?

En España, la protección de datos personales es un Derecho Fundamental* . Se regula en el Artículo 18.4 de la Constitución Española: “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

A nivel europeo, el artículo 8.1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

¿Por qué es importante?

Porque reconoce a cada persona la facultad de controlar sus datos y la capacidad de disponer y decidir sobre ellos.

*Los Derechos Fundamentales son todos aquellos derechos atribuibles a todas las personas sin excepción, y que se consideran como un listado de reglas básicas y preeminentes en el ordenamiento jurídico. Estos son notoriamente diferentes al resto de derechos porque son inalienables (se adquieren desde el nacimiento) y no pueden ser objeto de transacción o intercambio en el contrato de trabajo, aunque pueden sufrir alguna modulación por lo que el trabajador está subordinado y tiene dependencia del empresario.

Introducción

Marco normativo

- Europa: Nos encontramos, principalmente, con el Reglamento General de Protección de Datos (RGPD):
  - 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.

- España: Se destaca, entre otros, la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales. (LOPDGDD):
  - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

El objetivo de ambas leyes es dar un mayor control a los ciudadanos sobre su información privada en un mundo con cada vez más dependencia a los teléfonos inteligentes, a las redes sociales, a la banca por internet, al internet de las cosas, al big data y a las transferencias globales.

Tienen por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

También son de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Definiciones básicas

Interesado

Persona física identificada o identificable cuyos datos personales se tratan.

Datos especialmente protegidos o datos sensibles

Algunos de los datos personales son especialmente sensibles por revelar circunstancias o información de las personas sobre su esfera más íntima y personal. Requieren que se les preste una especial atención y se adopten las medidas técnicas y organizativas necesarias para evitar que su tratamiento origine lesiones en los derechos y libertades de los titulares de los datos. Son aquellos relacionados con la ideología, religión, afiliación sindical, creencias, salud, origen racial o étnico, vida sexual, datos genéticos y biométricos.

Tratamiento de datos

En la práctica, cualquier actividad en la que estén presentes datos de carácter personal constituirá un tratamiento de datos, ya se realice de manera manual o automatizada, total o parcialmente, 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, cotejo o interconexión, limitación, supresión o destrucción.

Introducción

Definiciones básicas

Tratamiento de datos (cont.)

Trato datos personales continuamente en mi trabajo diario. Cuando:

- Recojo datos de las personas usuarias de servicios.
- Gestiono datos de personal (nóminas, contratos, formación).
- Utilizo datos de personas de contacto (clientes, potenciales clientes, personal, proveedores, etc.).Facilito datos de las personas socias de mi entidad a terceros.

Delegado de Protección de Datos (DPD o DPO)

El Delegado de Protección de Datos es una figura clave en el modelo de su cumplimiento dentro de una empresa. Debe ser una persona conocedora del derecho y la práctica en materia de protección de datos.

Entre sus funciones se destacan la de informar y asesorar al responsable o al encargado del tratamiento (figuras que veremos a continuación) de las obligaciones que establece el RGPD y supervisar su cumplimiento, que ejerce de manera independiente. También es el punto de contacto con la AEPD.

The Bridge cuenta con un DPO, disponible ante cualquier duda o consulta relacionada con esta materia a través del siguiente correo electrónico: dpo@thebridgeschool.es

Responsable del tratamiento

El responsable del tratamiento es la persona física o jurídica, pública o privada, que se beneficia, necesita o decide sobre la finalidad, contenido y uso del mismo, directamente o porque así le viene impuesto por una norma legal.

Cada entidad (empresa, asociación, fundación, etc.) es responsable de los tratamientos de datos sobre los que decide. En este caso, The Bridge es responsable de los datos sobre los que decide cómo y para qué se lleva a cabo ese tratamiento.

- Un centro educativo es responsable de los datos de su alumnado.
- Una peluquería es responsable de los datos de las personas que asisten.
- Una entidad o empresa es responsable de los datos de su personal.

Encargado del tratamiento

El encargado del tratamiento es la persona física o jurídica, autoridad, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

En determinados casos, las escuelas para cumplir sus funciones necesitan contar con la colaboración de otras personas o entidades que no forman parte de su organización, por ejemplo, empresas que realizan las nóminas, el pago de impuestos, el servicio de limpieza, o todas aquellas actividades externalizadas.

Introducción

Definiciones básicas

Encargado del tratamiento (cont.)

Estas personas y entidades para prestar sus servicios también pueden tratar datos de carácter personal, por encargo del responsable del tratamiento, es decir, por parte de The Bridge en este caso. Las empresas que realizan este tipo de servicios tienen, en relación con el tratamiento de datos personales que realizan, la consideración de encargados de tratamiento.

Es obligatorio que el tratamiento de datos que implica la prestación del servicio se rija por un contrato que deberá incluir las garantías adecuadas:

- Seguir instrucciones del responsable: tratamiento y comunicaciones.
- Personas con acceso a datos: formación y compromisos de confidencialidad
- Medidas de seguridad: en función de la evaluación de riesgos
- Subcontratación. Se permiten subencargados, con autorización.
- Destino de los datos, al finalizar la prestación: supresión o devolución.
- Colaboración en el cumplimiento de las obligaciones del responsable:
    - Información, Consentimiento, Notificación de violaciones de seguridad, Derechos de interesados, Evaluaciones de Impacto de Privacidad
    - Colaboración para demostrar el cumplimiento: en auditorías, inspecciones

Agencia Española de Protección de Datos (AEPD)

La Agencia Española de Protección de Datos es la autoridad pública independiente, con presupuesto propio y plena autonomía funcional, encargada de velar por la privacidad y la protección de datos de la ciudadanía. Su objetivo es, por un lado, el de fomentar que las personas conozcan sus derechos y las posibilidades que la Agencia les ofrece para ejercerlos y, por otro, que los sujetos obligados tengan a su disposición un instrumento ágil que les facilite el cumplimiento de la normativa

Cuenta con una sede electrónica y con un conjunto de guías y publicaciones orientadas tanto a personas como a responsables

Derechos de los interesados

La normativa de protección de datos permite que los interesados ejerzan ante el responsable del tratamiento sus derechos de acceso, rectificación, oposición, supresión (“derecho al olvido”), limitación del tratamiento, portabilidad, de no ser objeto de decisiones individualizadas y de presentar reclamaciones ante la Agencia Española de Protección de Datos (AEPD).

- Acceso: derecho a dirigirse al responsable del tratamiento para conocer si está tratando o no datos de carácter personal del interesado y, en el caso de que se esté realizando dicho tratamiento, obtener información sobre dicho tratamiento (fines, categoría de datos, copia de los mismos, etc.).

Introducción

Definiciones básicas

Derechos de los interesados (cont.)

- Rectificación: permite al interesado obtener la rectificación de datos personales que sean inexactos sin dilación indebida del responsable del tratamiento.
- Oposición: la facultad del interesado de oponerse a que el responsable realice un tratamiento de sus datos personales.
- Supresión: derecho a que el responsable elimine los datos personales del interesado. Para ello tienen que concurrir ciertas circunstancias, como que los datos ya no sean necesarios en relación con los fines para los que fueron recogidos, o si han sido tratados de forma ilícita, entre otros.
- Limitación del tratamiento: derecho a que el interesado obtenga la limitación del tratamiento que el responsable hace con sus datos.
- Portabilidad: su finalidad es la de reforzar aún más el control de los datos personales del interesado, de forma que cuando el tratamiento se efectúe por medios automatizados, reciba sus datos personales en un formato estructurado, de uso común, de lectura mecánica e interoperable, y pueda transmitirlo a otro responsable del tratamiento, siempre que el tratamiento se legitime en base al consentimiento o en el marco de la ejecución de un contrato..
- No ser objeto de decisiones individuales automatizadas: pretende garantizar que el interesado no sea objeto de una decisión basada únicamente en el tratamiento de sus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre el interesado o le afecte significativamente de forma similar.
- Información: derecho del interesado a ser informado, por el responsable del tratamiento, sobre los datos personales que está recabando.
- Presentar reclamaciones ante la AEPD: cualquier interesado que tenga pruebas o indicios de un incumplimiento o infracción de la normativa de protección de datos que afecte al tratamiento de sus datos personales, puede presentar una reclamación ante la Agencia aportando dichos documentos..

Cookies

Una cookie es fragmento de código que se instalan en tu ordenador cuando visitas una página web. Da igual si estás entrando a la web desde el ordenador o desde el móvil, siempre se solicitará el almacenamiento de la cookie. Como normal general, en cumplimiento del RGPD. cuando accedes a una página web ésta te solicitará la utilización de cookies porque están obligadas a avisarte y a preguntarte cuáles quieres instalar.

Introducción

Definiciones básicas

Cookies (cont.)

Las cookies suelen utilizarse principalmente para dos finalidades principales: recordar accesos y conocer hábitos de navegación. Las cookies hacen que las páginas web puedan identificar tu ordenador, y por lo tanto, si vuelves a entrar en ellas podrán recordar quién eres y qué has hecho antes dentro de las mismas.

Existen diferentes tipos de cookies dependiendo de los fines para los que se utilicen, como por ejemplo: cookies técnicas, de funcionalidad, de seguridad, analíticas, de publicidad, de personalización, de análisis, de complementos, de reproductor multimedia, etc.

Infracciones y sanciones

El RGPD establece una serie de sanciones por el incumplimiento de sus disposiciones con multas de hasta 10 millones de euros (o el 2% de la facturación anual global del ejercicio anterior, aplicando la cuantía que resulte más alta), o en caso de infracciones muy graves, con multas de hasta 20 millones de euros (o el 4% de la facturación anual global del ejercicio anterior, aplicando la cuantía que resulte más alta).

Por su parte, la LOPDGDD clasifica las infracciones en leves, graves y muy graves, cada una de ellas con su correspondiente sanción..

Se consideran infracciones **leves**, entre otras, no atender las solicitudes de ejercicio de los derechos de los interesados (recordemos: derechos de acceso, rectificación, oposición, supresión (“derecho al olvido”), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas); incumplir la obligación del encargado de tratamiento de informar al responsable sobre un posible infracción por incumplir con el RGPD; notificar de forma incompleta, tardía o defectuosa a la AEPD sobre la información relacionada con una violación de seguridad de datos personales, etc.

Multas: multas de hasta 40.000 €.

Se consideran infracciones **graves**, entre otras, tratar datos de menores de edad sin su consentimiento (cuando tenga capacidad para ello), o el de sus padres o tutores; o la falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento.

Multas : entre 40.001 y 300.000 €.

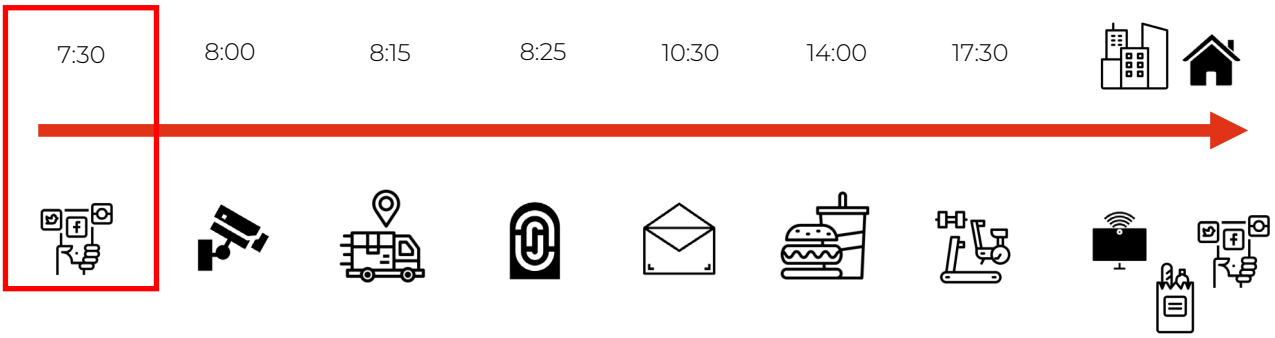
Se consideran infracciones **muy graves**, entre otras, vulnerar los principios y garantías relativos al tratamiento, por ejemplo, no tratar los datos de manera lícita, leal y transparente en relación con el interesado; utilizar os datos para una finalidad que no sea compatible con la aquella para la cual fueron recogidos,; la o misión del deber de informar al afectado acerca del tratamiento de sus datos personales; o la vulneración del deber de confidencialidad.

Multas: más de 300.001 €.

La Protección de Datos en nuestro día a día

A continuación, vamos a realizar un ejercicio práctico. Quiero que cada uno de nosotros pensemos en un día corriente de nuestras vidas, desde que nos levantamos hasta que nos acostamos. Con esto, vamos a ver la relación de nuestras actividades cotidianas con la protección de datos.

Analizamos una jornada por horas:



7:30:

Me despierto, me ducho y me tomo el café. Abro el móvil, reviso Whatsapp y alguna red social: Instagram, Facebook...

Meta, el conglomerado de empresas al que pertenecen las aplicaciones anteriores, recoge de todas ellas una gran cantidad de datos personales, reconocimiento facial, nuestros contactos en la agenda, nuestra geolocalización, acceden a nuestro listado de llamadas y mensajes, etc. Lo que entra en este universo no se borra y se vende a otras empresas, a pesar de las sanciones que a dicha empresa se le puedan imponer.


SANCIÓN

Protección de Datos multa a Google con 10 millones de euros por vulnerar el derecho al olvido

- También impone una multa a Vodafone España de 3,9 millones de euros

Si en el ámbito profesional nos exponemos ante este escenario y utilizamos aplicaciones como Whatsapp, por ejemplo, para enviar o recibir documentos de trabajo, éste, así como los datos que contiene, automáticamente acabará expuesto a la empresa anterior.


DATOS PERSONALES >

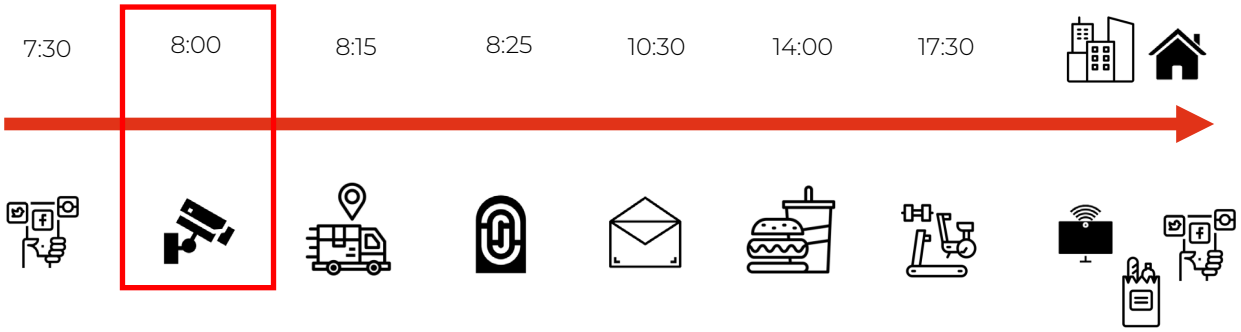
Multa de 225 millones a WhatsApp por no informar a sus usuarios de cómo compartía los datos con Facebook

La autoridad de protección de datos de Irlanda quintuplicó la sanción propuesta inicialmente, tras la presión de varios países europeos

RAFA DE MIGUEL

Por ello, no es recomendable utilizar este tipo de herramientas para enviar información confidencial. No obstante, en ocasiones puntuales, en las que no se traten datos confidenciales, su uso está permitido, por ejemplo, si se establece como canal para hablar con alumnos sobre un cambio de horario o para responder alguna duda, etc.

La Protección de Datos en nuestro día a día



8:00:

Salgo de mi casa y en el portal nos encontramos con un cartel en la puerta que nos avisa de que una cámara de seguridad está grabando todas nuestras entradas y salidas.

Aquí también se están exponiendo nuestros datos. Nuestra imagen, en la medida en la que nos identifique, constituye un dato de carácter personal que puede ser objeto de tratamiento para diversas finalidades. En este caso, se utiliza la cámara para garantizar la seguridad de los vecinos, los bienes y las instalaciones de nuestro edificio.

En el ámbito laboral, si uno de los profesores decide grabar la clase, ya sea presencial o vía online con la cámara, las imágenes solo podrán ser accesibles para las personas involucradas en la actividad, los profesores, los alumnos o sus padres o tutores en caso de menores de edad. Estas imágenes no se pueden colgar en internet, salvo que todas las personas que aparecen en ellas nos den su consentimiento expreso para utilizarlo con esa finalidad. En caso de incumplimiento de esta premisa la empresa, como responsable del tratamiento, podrá ser denunciada y sancionada.

La Protección de Datos en nuestro día a día

8:15:

Tengo una reunión a las 8:30 y no me da tiempo a coger el metro y llegar a tiempo a la oficina. Abro mi teléfono y entre mis aplicaciones encuentro diversas formas de dirigirme al trabajo: Uber, Cabify, Car2go, eCooltra, etc.

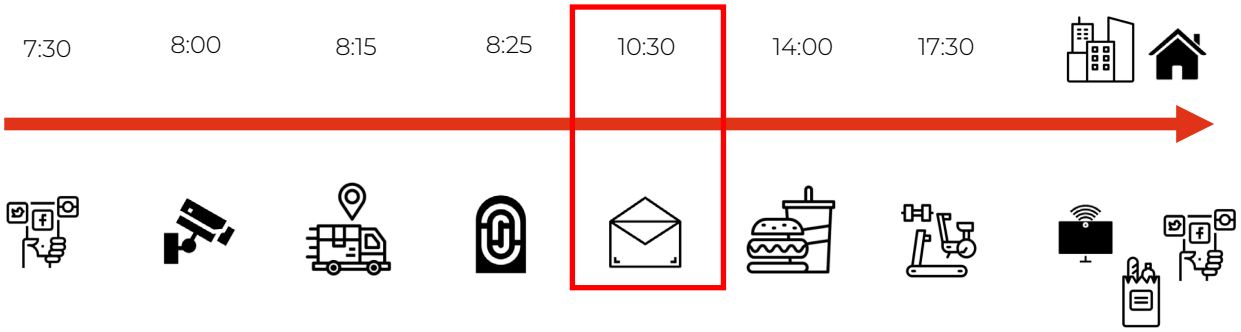
Todas estas aplicaciones recogen, entre otros, nuestros datos de geolocalización, es decir, conocen nuestra posición geográfica, las zonas en las que nos movemos, nuestros horarios, etc. Este tipo de empresas, pueden aprovechar esta información para enviarnos ofertas comerciales según nuestro lugar de residencia o, entre otros, para revender nuestras rutas, costumbres, etc. a otras empresas terceras que nos envíen publicidad directa 1to1.

8:25:

Llego a tiempo a la nueva oficina que acaba de alquilar la empresa. Para poder acceder a nuestro módulo, se solicita a la entrada nuestra huella dactilar.

En este caso, son mis datos biométricos (datos sensibles) los que se están recabando. Los datos biométricos son aquellos relativos a las características únicas del ser humano, que faciliten y garanticen la identificación de una persona. Son datos biométricos: las huellas dactilares, los patrones faciales, la retina, nuestra voz, el ADN, etc.

La Protección de Datos en nuestro día a día



10:30:

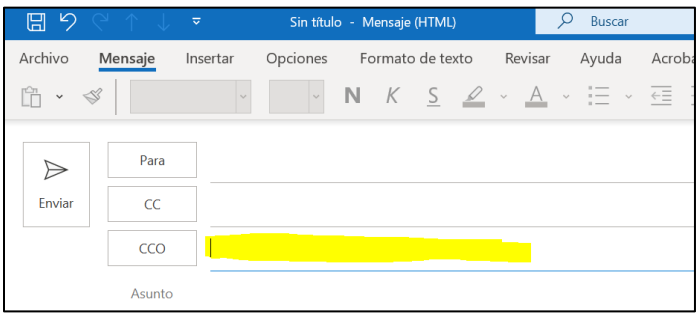
Termino mis reuniones y abro el correo. Empiezo a contestar a varios clientes / alumnos y decido convocar una reunión con varios de ellos para tratar un asunto importante.

En este caso, soy yo el que estoy manejando datos personales de terceros, en concreto los correos electrónicos. Para no tener ningún problema, y proteger los datos de mis clientes / alumnos, decido poner todos los correos electrónicos en CCO, para preservar su identidad.

Asimismo, hay que reseñar la importancia de que, en ningún caso, se recomienda el uso del correo personal para asuntos laborales, ya que no siempre están sujetos a las medidas de seguridad oportunas.

Tampoco es recomendable utilizar redes o internet de Wifi público, en general, y mucho menos en el ámbito laboral, porque podemos sufrir importantes robos de datos.

Por último, recalcar la importancia de reconocer aquellos correos maliciosos o estafas y no abrir nunca los archivos adjuntos que en ellos puedan aparecer. En caso de que recibas un correo de una cuenta desconocida, comprueba con precaución algún detalle que una entidad oficial nunca vaya a utilizar.



La Protección de Datos en nuestro día a día

14:00:

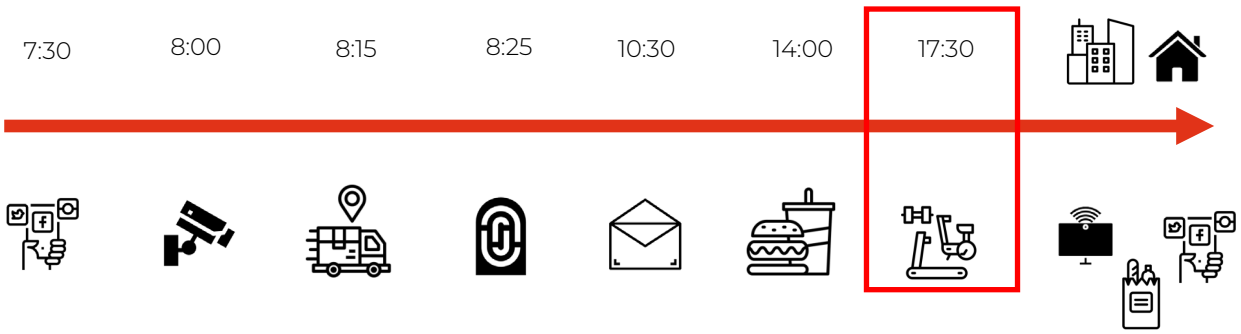
Continuo mi jornada y ya es la hora de comer. Con las prisas se me olvidó preparar comida para traer a la oficina y algunos compañeros decidimos salir a almorzar. Para agilizar el tiempo de espera en el restaurante, hemos decidido reservar a través de su web, aceptando su política de cookies e indicando nuestro correo electrónico y nuestro número de teléfono.

Algunos restaurantes, especialmente las cadenas grandes de restauración utilizan nuestros datos para conocer nuestros gustos, nuestros comportamientos, preferencias, hábitos, etc.

¿Os ha pasado alguna vez que el día o la hora en los que habitualmente no tienes ganas de preparar la cena, te empiezan a aparecer anuncios de comida rápida en páginas web en tu móvil o en tus redes sociales?

En mi caso la respuesta es sí.

La Protección de Datos en nuestro día a día



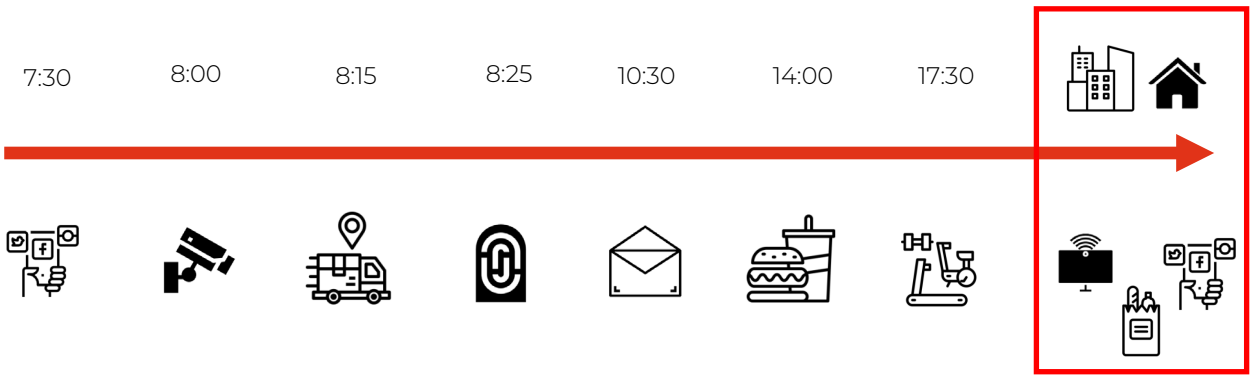
17:30:

Una vez terminada mi jornada laboral, me acerco a un gimnasio cercano, quiero empezar a adquirir hábitos saludables y voy a empezar por hacer deporte. Para poder registrarme, además de solicitar mi cuenta bancaria, me solicitan una serie de datos personales, algunos de ellos relacionados con mi estado de salud, con mis gustos y mi alimentación para poder prepararme unos ejercicios y una dieta acorde a mis necesidades. Les informo de que recientemente tuve una lesión en la rodilla y de que soy una persona alérgica a los frutos secos.

Este tipo de información, relacionada con la salud, se trata de un dato sensible especialmente protegido por el RGPD y por la LOPDGG.

¿Consideráis que el gimnasio al que me he apuntado cumple con la normativa y protege mis datos sensibles/especialmente protegidos? Sí, porque además de haber solicitado mi consentimiento expreso, el gimnasio cuenta con mayores medidas de seguridad para evitar pérdidas, alteraciones o accesos no autorizados en relación con estos datos sensibles.

La Protección de Datos en nuestro día a día



Vuelta a casa:

Después del gimnasio, vuelvo a casa con mucho cansancio. Me siento en el sofá y me pongo una serie en mi plataforma favorita. Como no, otra vez se están tratando mis datos personales, los cuales me solicitan para registrarme y acceder a las aplicaciones. Entro en la web de mi supermercado de confianza y hago un pedido de comida sana para cumplir con la nueva dieta, nuevamente están tratando mis datos personales. Ceno y me voy a la cama, no sin antes revisar varias aplicaciones de mi móvil.

Conclusiones

- La protección de datos está presente en la gran mayoría de nuestras acciones cotidianas, es una materia muy importante.
- Necesidad de regulación especial.
- Como posibles interesados debemos ser conscientes de nuestros derechos y ejercitarlos.
- Necesidad de cumplimiento por parte de las empresas y de adquirir buenas prácticas en la materia.
- Debemos tener precaución con aplicaciones gratuitas, especialmente en el ámbito laboral.

La Protección de Datos en nuestro día a día

Consejos

A continuación, se enumeran una serie de consejos para evitar la publicidad no deseada:

- Inscribe tus datos en la Lista Robinson, un fichero de exclusión publicitaria.
- Utiliza las fórmulas que ofrecen las empresas para rechaza el uso de datos con fines publicitarios.
- Evita dar tu consentimiento para que te envíen publicidad.
- Retira tu consentimiento.
- Ejerce tus derechos de oposición y supresión.
- Considera la mediación de AUTOCONTROL.
- Reclama ante la AEPD.

Buenas prácticas

Por último, se detallan una serie de buenas prácticas a cumplir por el personal de The Bridge:

1. Deber de secreto profesional y la confidencialidad respecto al uso, acceso o tratamiento de datos de los ficheros de la organización, incluso después de finalizada la relación laboral y/o mercantil con la organización. Puede ser considerada como una falta grave o muy grave.

2. Conocer y respetar las medidas de seguridad, y en especial, los derechos de acceso y límites respecto del uso de datos de carácter personal y respetar lo dispuesto en las políticas internas en la materia: Política Interna de Datos Personales y Política de Brechas de Seguridad, Política de Derechos ARCOPS.

3. Poner, inmediatamente, en conocimiento del DPO dpo@thebridgeschool.es cualquier recepción de solicitud de ejercicio de derecho ARCOPS. Asimismo, colaborar con el DPO, enviándole toda la documentación de la que dispongo y poniéndole en contacto con otras áreas que hayan podido tener acceso a los datos personales del interesado.

4. Ser responsable del puesto de trabajo asignado, respetando las medidas establecidas para impedir que personas no autorizadas accedan a datos de carácter personal. Crear contraseñas robustas y no compartirlas con ningún compañero, ni nadie externo a la organización.

5. En el uso de impresoras asegurarse de que no quedan documentos impresos, retirando los documentos a medida que vayan saliendo. Llevar a cabo una política de mesas limpias y custodia de armarios.

6. No cambiar la configuración de la conexión de los puestos de trabajo a redes o sistemas exteriores, salvo cuando esté autorizado expresamente.

7. No extraer información en ningún tipo de soporte sin autorización. Prohibido guardar copias sin autorización. Para el trabajo fuera del centro, no copiar ni transportar información de los sistemas centrales ni documentación en papel sin la correspondiente autorización.

8. Mientras los documentos no se encuentren archivados en los dispositivos de almacenamiento establecidos por la empresa, el responsable que se encuentre al cargo de los mismos, deberá custodiar e impedir en todo momento el acceso a personas no autorizadas.

Buenas prácticas

9. Para aquellos datos que deban ser transportados (ya sea físicamente o a través de redes públicas) activar la protección necesaria para evitar accesos no autorizados, utilizando contenedores adecuados, cifrado de los dispositivos, o utilización de canales de comunicación seguros.

10. Cuando se reciclen medios que sean reutilizables (digitales o papel), deberán ser borrados físicamente antes de su reutilización, para que los datos que contenían no sean visibles ni recuperables. Aquellos que no tengan que ser reutilizados deben ser destruidos de forma segura.

11. No se permite instalar programas informáticos sin autorización previa. Y en ningún caso, programas sin la debida licencia.

12. Es obligatorio comunicar las incidencias o anomalías de las que tenga conocimiento que afecten o puedan afectar a los datos o actividades de tratamiento de la empresa. El conocimiento y la no notificación de una incidencia por parte de un usuario será considerada como una falta grave contra la seguridad de la empresa.

13. Limitar el uso de los sistemas de comunicación (e-mail, teléfonos inteligentes, tabletas, etc.) al desarrollo de las funciones estrictamente asignadas al puesto de trabajo. Los activos y medios que pone la organización a disposición de los empleados (ordenadores, aplicaciones, correo, internet, etc.) son para uso profesional y deberán usarse de forma adecuada y para los fines profesionales requeridas.

14. No abrir archivos adjuntos de los mensajes de correo electrónico de origen desconocido, y evitar la descarga de archivos e instalación autoejecutables de programas de Internet, sin las suficientes garantías de seguridad sobre su origen e integridad.

15. Facilitar y canalizar el ejercicio de los derechos de los interesados. Por ello se informará inmediatamente a un responsable y se facilitará y recogerá siempre la solicitud escrita, identificando mediante DNI al interesado.

¡Muchas gracias!

He leído y comprendido lo dispuesto en esta formación en materia de protección de datos personales, comprometiéndome a la aplicación de lo dispuesto en la misma, dentro de mi ámbito laboral, en The Bridge School.

Nombre y apellidos:

Correo electrónico:

Firma: