T-Innova

Informe RGPD v1.1

La implantación de la nueva normativa de protección de datos (RGPD) trae consigo algunos cambios que afectan a la forma de conseguir, almacenar y gestionar la información.

1. Tipología de información:
    a. **Datos personales**: Nombre, dirección, email, datos bancarios, nacimiento, sexo, etc. Según la antigua LOPD corresponden a nivel 'básico' y son los que principalmente vamos a trabajar en este informe.
    b. Datos sensibles, especialmente protegidos o categoría especiales de datos: En este apartado se incluyen la **huella dactilar**, así como una **fotografía** del usuario.

        La RGPD obliga a

        i. Tener un consentimiento específico para cada tipo de datos protegido
        ii. Encriptar/cifrar esta información o almacenarla de forma independiente de manera que no esté relacionada con los datos personales.
        iii. Realizar un '**Registro de las actividades de tratamiento**', que, entre otras cosas, audita quien, cuando y a qué datos ha accedido.

            Las empresas de menos de 250 trabajadores no están obligadas a realizar dicho registro excepto si almacenan datos sensibles.

        "Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos"

    c. **Datos médicos:** Por ejemplo, PAR-Q. Cara al RGPD, están dentro de la categoría anterior, pero según la antigua LOPD, corresponden a nivel 'alto', por lo que es resulta muy complejo conseguir implantar las medidas de seguridad necesarias para cumplir los requerimientos marcados por la propia LOPD.

        Estamos a la espera de la versión revisada de la LOPD pero difícilmente será más laxa en este sentido.

        Lo más recomendable sería no almacenar este tipo de información o utilizar la 'seudonimización' (que estos datos se almacenen sin estar directamente relacionados con una persona, por ejemplo, con un número de expediente).

        "El RGPD no anula la LOPD, que continúa en vigor en las materias que aquél no regula"

d. **Información anónima**: Información que no guarde relación con una persona física, ya sea porque se ha suprimido parte de la información o porque se haya alterado. No se ve afectada por la RGPD. Por ejemplo, si suprimimos nombre, apellidos, DNI, teléfono, datos bancarios y email de la ficha de un cliente, pasaríamos a tener información anónima (pudiendo conservar datos como el sexo, fecha de nacimiento, servicios contratados, etc.)

"... por lo tanto, los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación."

2. Recogida de información:

Uno de los principales cambios de RGPD cara a la recogida de información es que el usuario ha de aceptar explícitamente el uso de dicha información y ha de poder autorizar de forma separada cada uso que se le vaya a dar a dicha información.

Sin embargo, *según lo establecido en la ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio electrónico y con la ley orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD) y el reglamento que la desarrolla (RD 1720/2007),* la comunicación con el usuario relacionada directamente con una vinculación contractual (por ejemplo, por haber contratado determinado servicio) no requiere autorización por parte de dicho usuario ni puede ser revocada. A efectos prácticos, eso quiere decir que no necesitamos autorización para enviarle una factura a un cliente por email o llamarle para reclamar una deuda pendiente.

Cada autorización solicitada ha de ser **libre** (no puede estar condicionada de ninguna forma), **específica** (se ha de utilizar para un fin concreto), **informada** (finalidad, responsable, tipo de tratamiento y derechos del usuario) e **inequívoca** (entendible y no ambigua).

Por ello, ya no es suficiente con una casilla 'Acepto las condiciones…' si no que hay que detallar la información vinculada a dicha autorización, aceptarla y firmarla. Por ejemplo:

☐ He leido y acepto las condiciones legales (*)

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS. Responsable: [EMPRESA] Finalidades: a) Actividades comercial por distintos medios y canales de comunicación de iniciativas y servicios de entidades propias y colaboradores. b) Gestionar las solicitudes relacionadas con cualquier iniciativa de entidades propias y colaboradores. Legitimación: Consentimiento del interesado. Destinatarios: Se prevé, en su caso, la comunicación de los datos del interesado a la entidad [EMPRESA] responsable de la actividad solicitada. Derechos: Tiene derecho a acceder, rectificar y suprimir los datos u oponerse al tratamiento de los mismos o a alguna de las finalidades, así como otros derechos, como se explica en la información adicional. Información adicional: Puede consultar la información adicional y detallada sobre Protección de Datos al link de política de privacidad.

Estas condiciones resumidas se denominan '**capa 1**' y tienen que permitir acceder mediante un enlace a las condiciones completas (**capa 2**), por ejemplo: https://fundaciocet10.org/es/aviso-legal

Por 'capa 0' entenderemos el consentimiento en sí (el literal de la pregunta). Por ejemplo: *¿Aceptas el envío de comunicaciones comerciales?*

3. Supresión de datos personales

"...el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando (...), entre otros casos, los datos personales ya no sean necesarios en relación a los fines para los que fueron recogidos o tratados de otro modo".

La cancelación de los datos es un procedimiento divido en 2 fases: la primera de marcado y bloqueo del dato, y la segunda consistente en su borrado o eliminación física.

- Bloqueo del dato: El dato se mantendrá, pero solo será accesible a perfiles y condiciones muy concretas

  "La cancelación de los datos no supone su eliminación automática, sino su bloqueo tal y como dispone el artículo 16.3 de la Ley Orgánica 15/1999".

  *En su informe de 5 de junio de 2007 la AEPD indicaba que "*deberá efectuarse de forma tal que no sea posible el acceso a los datos por parte del personal que tuviera habitualmente tal acceso, por ejemplo, el personal que preste sus servicios en el centro consultante, limitándose el acceso a una persona con la máxima responsabilidad y en virtud de la existencia de un requerimiento judicial o administrativo a tal efecto. De este modo, pese a permanecer el tratamiento de los datos, el acceso a los mismos quedaría enteramente restringido a las personas a las que se ha hecho referencia.

  El artículo 5.1.b) del Reglamento de desarrollo de la LOPD 15/1999 (Real Decreto 1720/2007), define el concepto de cancelación en los siguientes términos: "Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos."

- Borrado del dato: Una vez superado el plazo en el que el dato ya no es necesario, se ha de proceder a su borrado definitivo.

4. Adaptación DeporWin al RGPD:
    a. Nuevas casillas de consentimiento: Para cada consentimiento informado, ha de existir el correspondiente registro en la ficha de la persona. Podemos identificar los siguientes tipos de consentimiento:
        i. Comunicaciones administrativas: Todas las vinculadas directamente con los servicios contratados. Como hemos visto en el punto 2, no es necesario consentimiento para este tipo de comunicaciones.
        ii. Comunicaciones comerciales: Envío de información publicitaria
        iii. Registro huella: Acepta que se almacene los datos biométricos de huella en el sistema
        iv. Registro fotografía: Acepta que se almacena la fotografía del usuario en el sistema
        v. Exportación de datos a terceras empresas (Technogym, MyVitale, Trainingym, etc.). Un consentimiento por cada exportación.

    En el caso de que solo haya un consentimiento informado para comunicaciones comerciales, se puede seguir utilizando el check actual (enviar correo).

    b. Recogida informada del consentimiento: En el caso de recoger el consentimiento mediante un medio electrónico (un panel de firma o una Tablet, por ejemplo), hay que mostrar el consentimiento y la capa 1 (condiciones resumidas de dicho consentimiento)

    c. Registro explícito del consentimiento: En el momento que el usuario nos consienta determinado uso de la información, se ha de registrar de forma fehaciente dicha aceptación. Esto puede ser mediante el escaneo de un documento manuscrito y firmado por el usuario o mediante un registro electrónico (Time Stamp Certified), en cuyo caso se ha de recoger la fecha/hora de la aceptación, así como almacenar la capa 1 y capa 2 vigentes en el momento de dicha aceptación.

    d. Operativa con las casillas de consentimiento de comunicación: En el momento de lanzar una comunicación, el sistema ha de saber qué tipo de comunicación es (administrativa o comercial) y filtrar el envío en función de cada autorización.

    Todas las casillas tienen que estar desmarcadas por defecto y el literal del campo tiene que estar expresado en positivo (no son válidos literales como 'Marque esta casilla si no desea que…')

    En cada etapa de envío de email de una campaña CRM hay que poder configurar el tipo de comunicación.

    En los procesos automáticos vinculados a un listado hay que poder definir qué tipo de comunicación es.

    Al enviar manualmente un correo electrónico hay que indicar si es administrativo o comercial (y qué tipo de comunicación comercial)

e. En cualquier comunicación comercial por correo electrónico se ha de incluir la opción de darse de baja o modificar las preferencias de suscripción del usuario.

f. En el caso de no aceptar el registro de la fotografía digital, no permitir capturar ni almacenar la fotografía del usuario

g. En el caso de no aceptar el registro de datos biométricos, no permitir capturar ni almacenar los datos biométricos del usuario

h. Una instalación puede decidir hacer obligatorios el registro de fotografía y datos biométricos por lo que, en este caso, estas casillas podrían estar activadas por defecto.

i. Proceso masivo de recogida de consentimientos: A través del módulo de boletines poder hacer un envío masivo (a partir de un listado) para que los usuarios puedan confirmar sus preferencias.

j. Borrado de información:

    i. Opción de bloqueo de información según el cual, los datos se han de ocultar de forma que solo un administrador tenga acceso a ellos.

    ii. Opción para la supresión de la información de los datos personales y biométricos de un usuario. Esto incluye no solo los datos de su ficha si no la información histórica y documentos adjuntos. Esta opción de borrado ha de ir suficientemente protegida para que no se pueda hacer un uso accidental.

5. Adaptación DeporWeb/DeporSite al RGPD:

   a. En la pantalla de alta de datos personales, se tienen que mostrar tantos consentimientos informados (incluyendo Capa 1 con su enlace a la Capa 2) como sean precisos.

   b. Se tiene que registrar en la base de datos cada consentimiento aceptado (o des-aceptado en el caso de modificar las preferencias) indicando la IP, fecha/hora/segundo, capa 1 y capa 2. Opcionalmente se puede incorporar una marca de tiempo de un proveedor TSA (por ejemplo https://www.safestamper.com/tsa) así como firmar dicha información con una firma digital.

   c. Se puede suprimir el consentimiento genérico ('acepto las condiciones de servicio…') actualmente necesario para continuar el proceso de alta

6. Miscelánea:

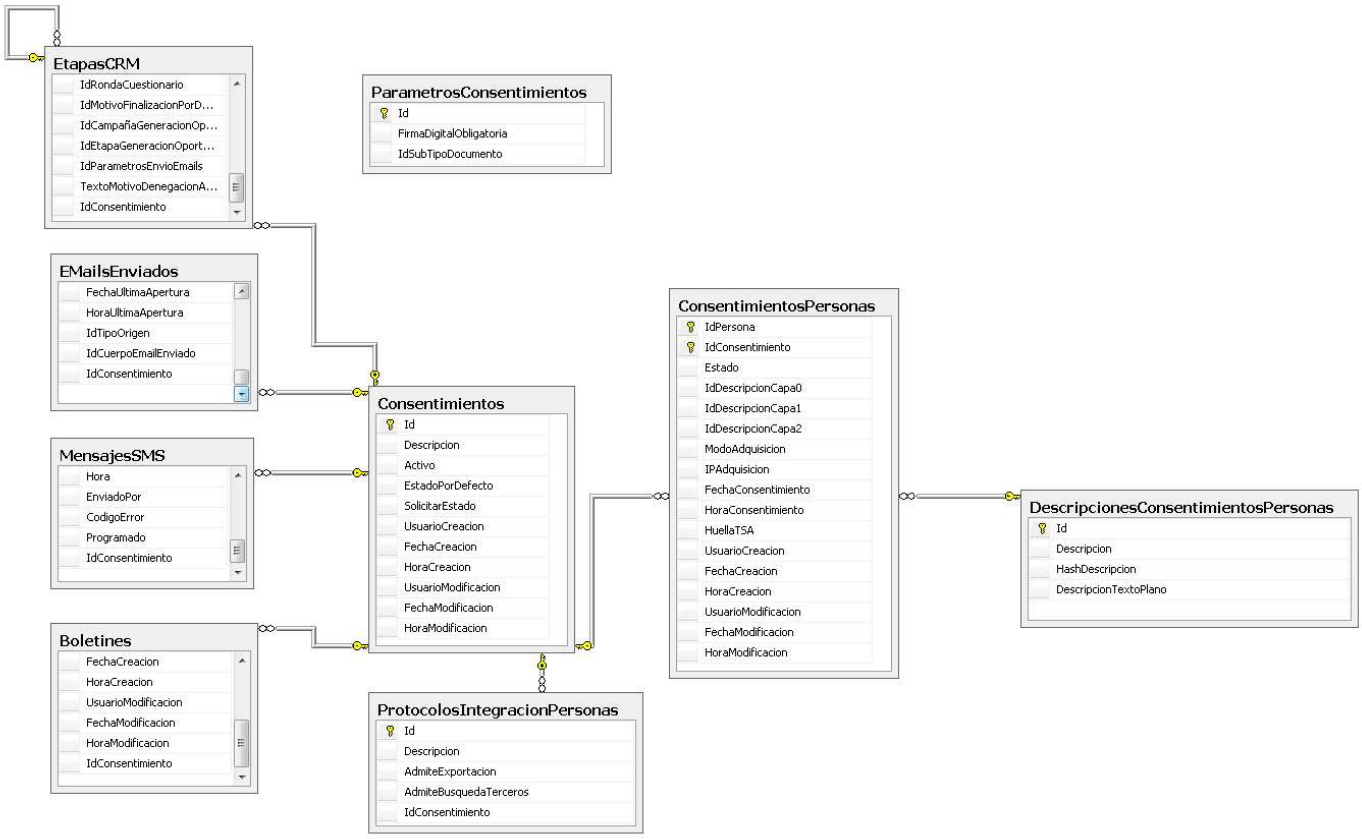
   a. La RGPD y la antigua LOPD no prevén sanciones económicas a la administración pública.

      Asimismo, la referida normativa vino a definir el procedimiento de resolución de las infracciones en materia de protección de datos que fueran cometidas por las administraciones públicas. En este sentido, en los casos de incumplimiento por parte de la administración, procederá el dictado de una resolución por parte de la Agencia Española de Protección de Datos, que será comunicada al responsable del fichero, al órgano del que dependa jerárquicamente y, en su caso, a los afectados, determinando qué medidas procederá adoptar para la cesación o corrección de los efectos de la infracción. Es decir, que los posibles incumplimientos de las administraciones públicas en materia de protección de datos, se resolverían sin imponer sanción pecuniaria alguna, sino imponiendo una "mera" adopción de medidas correctoras.

   b. Interés legítimo: Es un mecanismo (controvertido) que permite justificar el uso de información personal de forma unilateral sin consentimiento del interesado.

      https://jorgegarciaherrero.com/interes-legitimo-en-el-rgpd-y-iii-concepto-ventajas-y-riesgos/

Notas de diseño:



1. **Definición de consentimientos**

   - Definimos una nueva entidad ‘consentimientos’ en la que definimos los distintos tipos de consentimientos que nos puede aceptar el cliente.
   - Dentro de esta tabla, habrá varios registros de sistema (predefinidos por la aplicación):
     - **Consentimiento administrativo**: Para comunicaciones relacionadas con los servicios contratados por el cliente. En un principio, para este tipo de comunicados no se requiere consentimiento explícito por lo que se podrá configurar como aceptado por defecto y no solicitable.
     - **Comunicación comercial**: El sistema está preparado para poder definir diferentes tipos de comunicados comerciales. Por defecto, incorporará un tipo de comunicado comercial genérico que reemplazará al actual ‘EnviarCorreo’ (en la migración al modelo RGPD, habrá una opción de ‘heredar’ el valor de este campo). Por defecto no estará marcado y será solicitable al cliente.
     - **Registro biométrico:** En el caso de utilizar sistemas de huella 1:n (Sagem, STS3015, Kimaldi o Sigma BIO) en los que la huella se almacena en el sistema, se activará este consentimiento sin el cual no se permitirá el registro de la huella del cliente
     - **Fotografía:** Este consentimiento autoriza a almacenar la fotografía del usuario. Sin él, el sistema no permitirá guardar la fotografía en la base de datos.

- **Protocolos de exportación**: Se definirá un consentimiento para cada protocolo de exportación (Technogym, Traininigym, MyVitale, etc.)

- El consentimiento (Capa 0, 1 y 2) será multi-idioma y tendrá versión HTML (para consentimiento Web) y versión texto (para tableta y para imprimir el comprobante). Para evitar redundancia, la versión texto se podrá extraer de la versión HTML.

2. **Recogida de consentimientos**

- Para la recogida del consentimiento, se definirá un nuevo 'Tipo de Paso' en el motor de procesos automáticos: "Lanzar consentimiento". Esto permitirá solicitar consentimientos de forma automática (por ejemplo, al dar de alta la ficha de un cliente) o manualmente con una opción en la ficha de la persona.
- Manualmente se podrá desmarcar un consentimiento en cualquier momento (toda la información quedará registrada en el sistema)
- Al marcar un consentimiento manualmente, el sistema ofrecerá la posibilidad de solicitarlo mediante la Tablet o aceptar la entrada manual por parte del operador (en este caso, quedará marcado como consentimiento entrado manualmente)
- En v3/DeporNet se podrá limitar la aceptación manual de un consentimiento a través de restricciones funcionales.
- En el Historial se registrará las modificaciones de cualquier consentimiento.
- Para recoger un consentimiento presencial, se ha optado por incorporar una Tablet (por ejemplo, un iPad) al sistema ya que nos permitirá mostrar el contrato y consentimientos y recoger las diferentes aceptaciones y firma en un solo paso.
- La aceptación de un consentimiento por parte del cliente se registrará en el sistema, almacenando en modo texto (no HTML) la Capa 0 (literal del consentimiento), la Capa 1 (consentimiento resumido) y Capa 2 (consentimiento completo), fecha/hora, dirección IP (para consentimientos Web), HuellaTSA, operador y modo de adquisición (web, tableta, manual).
- Para optimizar espacio en la Base de Datos, los textos de los consentimientos aceptados se guardarán en una nueva tabla (DescripcionesConsentimientosPersonas) de forma que el texto solo se almacenará una vez. En el caso que se modifique un consentimiento se creará un nuevo registro.
- A través del motor de boletines se podrá recoger consentimientos de forma masiva. El motor de boletines podrá enviar emails con enlaces personalizados para que cada cliente pueda modificar sus consentimientos.
- Para clientes que no tengan DeporSite, T-Innova ofrecerá una página Web genérica donde se puedan recoger y validar los consentimientos (tanto para consentimientos Web como para consentimientos a través de una Tablet).

3. **Validación de consentimientos**

- En diversos procesos del sistema se validará previamente si existe la autorización pertinente por parte del cliente. En la muchos de ellos, se tendrá que configurar qué tipo de consentimiento requiere (sobre todo los consentimientos comerciales). Por defecto, el sistema configurará los siguientes consentimientos:
    - **Listados:** Por defecto, todos los listados se marcarán como 'proceso administrativo'. En el caso de que un listado se utilice para un comunicado comercial, se tendrá que modificar manualmente.
    - **CRM:** Todas las etapas de envío de email de cualquier campaña CRM se marcarán como 'comunicado comercial'. En el caso de que una campaña CRM se utilice como proceso administrativo, se tendrá que modificar manualmente. En el caso de que haya varios tipos de comunicación comercial, se tendrán que modificar manualmente las diferentes campañas para indicar qué tipo de comunicado comercial.
    - **Boletines:** Todos los boletines se marcarán como 'comunicado comercial' por defecto. En el caso de que sea comunicado administrativo o haya más de un tipo de comunicado comercial, se tendrá que modificar manualmente.
- La validación del consentimiento se realizará en el momento de ejecutar el envío (tanto de email como de SMS). Eso permite asegurar que disponemos del consentimiento adecuado justo en el momento de lanzar el envío.

4. **Seguridad**

- Los datos biométricos actualmente ya se almacenan de forma cifrada en la base de datos
- Las fotografías no se almacenan cifradas pero si se almacenan de forma separada a la base de datos principal tal y como recomienda el RGPD