IMPACTO DEL RGPD EN MI NEGOCIO

BILBAO 26 DE ABRIL DE 2018

1.- NUEVO MODELO DE PRIVACIDAD

Mismo marco para toda la UE. Modelo anglosajón.

Derogación de la Directiva 95/46/CE.

Aplicable directamente desde el 25/5/18.

Concurrencia de la LOPD, RLOPD y RGPD. PLOPD.

1.- NUEVO MODELO DE PRIVACIDAD

Principio básico que debe regir en todas las fases del tratamiento: la **responsabilidad proactiva**. Hay que cumplir y demostrar que cumple con el RGPD.

Analizar que datos se tratan, sus finalidades, los tratamientos para determinar la forma en que aplicarán las medidas técnicas y organizativas apropiadas a fin de **garantizar** que cumple el RGPD y **poder demostrarlo** ante los interesados y las autoridades en protección de datos.

Exige una actitud consciente, diligente y proactiva frente a todos los tratamientos que lleven a cabo.

1.- NUEVO MODELO DE PRIVACIDAD

Privacidad desde el diseño: antes de iniciar los tratamientos, deben definirse las operaciones de tratamiento y los medios para cumplir los principios y obligaciones del RGPD

Privacidad por defecto: aplicar medidas técnicas y organizativas para garantizar por defecto que sólo se tratan los datos necesarios, no conservarlos más tiempo del necesario y garantizar su seguridad.

Aproximación a la protección de datos desde el riesgo: medidas de seguridad.

Registro de actividades de tratamiento.

1.- NUEVO MODELO DE PRIVACIDAD

Evaluaciones de impacto del tratamiento para los derechos y libertades (EIDP).

Delegado de Protección de Datos (DPO)

Sanciones de 10.000.000 € o del 2% del volumen de negocio total anual global del ejercicio anterior optándose por la mayor cuantía o sanciones de 20.000.000 € o del 4% del volumen de negocio total anual global del ejercicio anterior optándose por la mayor cuantía.

Derecho a recibir una indemnización por daños y perjuicios materiales o inmateriales como consecuencia de una infracción del RGPD.

2.- ¿NECESITO EL CONSENTIMIENTO PARA TRATAR LOS DATOS?

Es toda manifestación de voluntad **libre, específica, informada** e **inequívoca** por la que el interesado acepta el tratamiento de los datos.

Forma: una clara acción afirmativa como, por ejemplo, marcar una casilla de una web, escoger parámetros técnicos para la utilización de servicios de la SI, el movimiento físico del teléfono, grabaciones de voz.

No el silencio, la inacción, las casillas ya marcadas.

El tratamiento sólo será lícito si se dio el consentimiento para uno varios **fines específicos (art.6.1 RGPD)**. Y deberá ser **explícito** para el tratamiento de **categorías especiales de datos** (art.9.2ª RGPD).

2.- ¿NECESITO EL CONSENTIMIENTO PARA TRATAR LOS DATOS?

Consentimiento de los menores de edad: RLOPD **mayores de 14** pueden otorgar el consentimiento.

Supuesto especial RGPD: consentimiento de menores en relación con la oferta directa de servicios de la sociedad de la información, **mayores de 16**.

RGPD que los estados podrán establecer una edad inferior para estos fines pero no inferior a 13 años. PLOPD.

El RT esfuerzos razonables para verificar si el consentimiento ha sido dado por el titular de la patria potestad o tutor del menor.

2.- ¿NECESITO EL CONSENTIMIENTO PARA TRATAR LOS DATOS?

Libre: debe suponer una verdadera elección y control por parte del interesado.

Si se incluye como una parte no negociable de los términos y condiciones se presume que **no se ha otorgado libremente.**

Ejemplo, app de edición de fotografía que solicita tener acceso a su localización GPS para el uso de la app y que usará sus datos con fines publicitarios.

Desequilibrio de poder. Si no puedes rechazar porque está presionado. Contexto laboral. Buscar otra base legítima.

2.- ¿NECESITO EL CONSENTIMIENTO PARA TRATAR LOS DATOS?

Condicionado. Vincular el cumplimiento de un contrato o la prestación de un servicio al consentimiento para el tratamiento de **datos que no son necesarios** se presume no válido.

Por ejemplo, si un banco solicita consentimiento para usar los datos de pagos con fines de publicidad y supedita sus servicios a aceptarlo.

Granulidad. Se presume no valido si no se puede autorizar por separado las distintas operaciones de tratamiento.

Por ejemplo, si se pide consentimiento para el envío de comunicaciones comerciales y también para compartir información entre empresas del grupo teniendo que aceptar las dos.

2.- ¿NECESITO EL CONSENTIMIENTO PARA TRATAR LOS DATOS?

Específico. Se concede para unos fines determinados. Si se quiere usar para otros fines distintos hay que recabar de nuevo el consentimiento.

Informado. (Principio de transparencia).

RT demostrar que el interesado consintió.

Revisión de los consentimientos para asegurar que están otorgados conforme al RGPD.

3.- TRATAMIENTOS QUE NO NECESITAN EL CONSENTIMIENTO

Cuando el tratamiento es necesario para la **ejecución de un contrato** en el que el interesado es parte o para la aplicación de medidas precontractuales.

Esta base jurídica no sirve para tratar datos de categorías especiales.

Es necesario para el cumplimiento de una **obligación legal** aplicable al responsable del tratamiento. Una norma del derecho de la Unión o una Ley.

Se aplica a las categorías especiales de datos en el ámbito del derecho laboral, SS y protección social

3.- TRATAMIENTOS QUE NO NECESITAN EL CONSENTIMIENTO

Es necesario para la satisfacción de un **interés legítimo** del RT siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado.

AGPD: Centros educativos no universitarios: comunicación de las notas a los padres cuando éstos se hacen cargo del pago.

Hay que realizar una evaluación meticulosa ponderando los intereses del RT y los derechos y libertades del interesado, **documentar la evaluación** y dar transparencia y visibilidad a esta información.

Cuestiones a valorar: si el interés es legítimo, real, actual (no especulativo);si es necesario; que interés prevalece; adoptar medidas adicionales, etc.

4.- CUMPLIR CON EL PRINCIPIO TRANSPARENCIA

Exige que toda información que se dirija al público o al interesado sea concisa, fácilmente accesible, fácil de entender, en leguaje claro y sencillo.

Para que un tratamiento sea lícito y leal tiene que quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que le conciernen.

Incidencia directa sobre el consentimiento (debe ser informado).

Adaptar la información al RGPD.

4.- CUMPLIR CON EL PRINCIPIO TRANSPARENCIA

En el momento en que obtengan los datos se debe informar de:

- La identidad y los datos de contacto del RT y, en su caso, de su representante.
- Los datos de contacto del DPO
- Los fines del tratamiento a que se destinan los datos
- La base jurídica del tratamiento

4.- CUMPLIR CON EL PRINCIPIO TRANSPARENCIA

- Si está basado en el interés legítimo
- Los destinatarios o categorías de destinatarios
- La intención de transferir datos a un tercer país u organización internacional
- El plazo durante el que se conservarán los datos o, cuando no sea posible, los criterios utilizados para determinarlos

4.- CUMPLIR CON EL PRINCIPIO TRANSPARENCIA

- El derecho a solicitar el acceso a los datos, la supresión, rectificación, limitación del tratamiento, portabilidad de los datos u oposición.
- El derecho a retirar el consentimiento
- El derecho a presentar una reclamación ante la autoridad de control
- Si la comunicación de datos es un requisito legal o contractual o un requisito necesario para suscribir un contrato

4.- CUMPLIR CON EL PRINCIPIO TRANSPARENCIA

- Si el interesado está obligado a facilitar los datos y las consecuencias de no facilitarlos

- La existencia de decisiones automatizadas, incluida la elaboración de perfiles

RT debe tener en cuenta todas las circunstancias de la recogida y el tratamiento al momento de decidir la modalidad o el formato apropiado para ofrecer la información

4.- CUMPLIR CON EL PRINCIPIO TRANSPARENCIA

La AGPD ha publicado una guía para el cumplimiento del deber de informar E:\IRUDILAB\GUIA INFORMACION AGPD.pdf

Propone ofrecer la información por capas o niveles.

Un primer nivel con la información básica resumida con los datos del RT, la finalidad, la legitimación, los destinatarios y los derechos.

Un segundo nivel con toda la información ya más detallada.

4.- CUMPLIR CON EL PRINCIPIO TRANSPARENCIA

Presentar la información de manera eficiente y sucinta para evitar el exceso y fatiga de información

Debe diferenciarse claramente de otra información no relacionada con la PD, como por ejemplo, las condiciones contractuales.

Si el interesado son niños, adecuar el lenguaje para que lo comprendan.

Redactarse en voz activa. No el “puede”, “podría”, “algunos”, etc.

5.- RELACIONES CON TERCEROS QUE PARA PRESTARME UN SERVICIO ACCEDEN A LOS DATOS

ET son las personas físicas o jurídicas, autoridades públicas, servicio u otro organismo que trata datos por cuenta del RT.

Ejemplos, proveedores de servicios de alojamiento de datos en internet, asesorías laborales, empresa destrucción de documentos, etc.

La cuestión clave para saber si nos encontramos ante un ET o un RT es que **es el RT quien decide sobre la finalidad** y los usos de la información, mientras que el ET trata los datos cumpliendo con las instrucciones de quien le encomienda un determinado servicio.

5.- RELACIONES CON TERCEROS QUE PARA PRESTARME UN SERVICIO ACCEDEN A LOS DATOS

El tratamiento por el ET se regirá por un **contrato** que vincule al ET respecto del RT y establezca el objeto, la duración, la naturaleza y finalidad del tratamiento, el tipo de datos y categorías de interesados y las obligaciones y derechos del RT. Y, en particular, deberá contener:

- Las instrucciones documentadas del RT
- Compromiso de las personas autorizadas para tratar los datos de respetar la confidencialidad.
- Tomar las medidas de seguridad necesarias

5.- RELACIONES CON TERCEROS QUE PARA PRESTARME UN SERVICIO ACCEDEN A LOS DATOS

- No subcontratar servicios de otro ET sin autorización previa por escrito del RT
- Asistir al RT para que pueda cumplir con las obligaciones de atención a los derechos de los usuarios.
- Ayudar al RT a cumplir con la obligación de seguridad y realización de EIPD
- A elección del RT suprimirá o devolverá todos los datos una vez termine la prestación y suprimirá las copias existentes salvo que esté obligado a conservarlos por ley.

5.- RELACIONES CON TERCEROS QUE PARA PRESTARME UN SERVICIO ACCEDEN A LOS DATOS

- Poner a disposición del RT toda la información necesaria para demostrar el cumplimiento de las obligaciones del RGPD y permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del RT u otro auditor autorizado por el RT

Directrices para la elaboración de contratos entre RT y ET en E:\IRUDILAB\GUIA CONTRATOS.pdf

El RT no pierde su condición por hacer un encargo de tratamiento.

Si se autoriza la subcontratación, el subencargado debe estar sujeto a las mismas condiciones y en la misma forma que el primer ET.

5.- RELACIONES CON TERCEROS QUE PARA PRESTARME UN SERVICIO ACCEDEN A LOS DATOS

Si se autoriza la subcontratación, el subencargado debe estar sujeto a las mismas condiciones y en la misma forma que el primer ET.

Sólo contratar con ET que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme al RGPD, y garantice la protección de los derechos del interesado.

La adhesión a un código de conducta del art.40 o a un mecanismo de certificación del art.42 RGPD.

Adaptación de los contratos al RGPD.

6.- QUE DERECHOS TIENEN LOS TITULARES DE LOS DATOS

Derechos ARCO más del de portabilidad, limitación del tratamiento y no toma de decisiones individuales automatizadas.

Facilitar la información en el plazo de 1 mes de la recepción de la solicitud, prorrogable 2 meses más en función de la complejidad y el número de solicitudes informando de ello al interesado.

Si pasado 1 mes no atiende el derecho el RT debe informar de las razones de su no actuación y de la posibilidad de acudir a la AGPD.

6.- QUE DERECHOS TIENEN LOS TITULARES DE LOS DATOS

Acceso: derecho a obtener confirmación de si se están tratando o no datos de carácter personal que le conciernen, y si se están tratando, acceder conocer que categorías de datos, la finalidad del tratamiento, los destinatarios, el plazo de conservación.

Rectificación: derecho a rectificar los datos inexactos y a completar los datos que sean incompletos.

Supresión: derecho a obtener sin dilación indebida la supresión de los datos cuando no son necesarios para la finalidad para la que se recogieron, cuando retire el consentimiento en los casos en los que es la única base legítima del tratamiento, etc.

6.- QUE DERECHOS TIENEN LOS TITULARES DE LOS DATOS

Limitación del tratamiento: derecho a que no se tratan sus datos **cuando se haya ejercido el derecho de rectificación mientras se determina si procede o no,** el tratamiento sea **ilícito** y el interesado se opone a la supresión de los mismos, ya no sean necesarios pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o defensa de reclamaciones y cuando se haya opuesto al tratamiento y se está verificando si procede.

Portabilidad: es el derecho a obtener los datos en un formato estructurado, de uso común y lectura mecánica cuando el tratamiento sea **automatizado,** este basado **en el consentimiento o en un contrato.**

6.- QUE DERECHOS TIENEN LOS TITULARES DE LOS DATOS

Son derechos gratuitos salvo cuando se formulen solicitudes manifiestamente infundadas o excesivas o repetitivas.

Atender en el plazo de 1 mes desde la recepción de la solicitud, prorrogable a 2 meses más en casos complejos.

Si no atiende se debe informar de los motivos y de la posibilidad de reclamar ante la AGPD y ejercer acciones judiciales

Importante: verificar la identidad del solicitante.

7.- REGISTRO DE FICHEROS EN LA AGPD VS REGISTRO DE ACTIVIDADES

Para demostrar la conformidad con el RGPD, el RT y el ET debe mantener registros de tratamientos bajo su responsabilidad.

Corresponde al RT decidir el nivel de agregación o segregación del registro.

Registro actividades de tratamiento cuando mas de 250 empleados, a menos que el tratamiento entrañe un **riesgo** para los derechos y libertades; **no sea ocasional**; **o incluya categorías especiales de datos** o datos relativos a condenas e infracciones penales.

En la práctica muy recomendable para dar cumplimiento al principio de responsabilidad proactiva.

7.- REGISTRO DE FICHEROS EN LA AGPD VS REGISTRO DE ACTIVIDADES

- nombre y datos de contacto del responsable y del DPO.
- los fines del tratamiento.
- una descripción de las categorías de interesados y de las categorías de datos.
- las categorías de destinatarios a quienes se comunican o comunicarán
- las transferencias internacionales a un tercer país
- cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos
- cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

8.- ¿QUÉ MEDIDAS DE SEGURIDAD TENGO QUE IMPLANTAR?

Antes se adoptaban en función del tipo de datos E:\IRUDILAB\MEDIDAS DE SEGURIDAD AGVPD.pdf y E:\IRUDILAB\MEDIDAS DE SEGURIDAD AGVPD NO AUTOMATIZADOS.pdf

Ahora, las que sean necesarias en función del riesgo al que están sometidos los datos.

Realizar un análisis de riesgos a los que están sometidos los tratamientos. Identificar los activos, sus amenazas, valorar el impacto, aplicar medidas, volver a valorar el impacto, revisar

Muchas metodologías de análisis de riesgos E:\IRUDILAB\GuíaAnalisisDeRiesgosRGPD.pdf

9.- ¿TENGO QUE NOTIFICAR INCIDENTES DE SEGURIDAD?.

Obligación del RT de notificar a la AGPD las violaciones de seguridad a más tardar en las 72 h siguientes a tener conocimiento de ello.

Obligación del ET de notificar al RT las violaciones de seguridad

Es toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado.

9.- ¿TENGO QUE NOTIFICAR INCIDENTES DE SEGURIDAD?.

Establecer un procedimiento de detección y actuación ante violaciones de seguridad.

No hay obligación de notificar si la violación de seguridad no constituye un riesgo para los derechos y libertades.

Evaluar el impacto y las consecuencias para los derechos y libertades

Si se concluye que hay riesgo, notificarlo a la AGPD y si hay un alto riesgo, notificarlo también a los interesados.

9.- ¿TENGO QUE NOTIFICAR INCIDENTES DE SEGURIDAD?.

Describir la naturaleza de la violación, con las categorías y números de afectados, y las categorías y número aproximado de registros afectados

Comunicar el nombre y los datos de contacto del DPO

Describir las posibles consecuencias y las medidas adoptadas o propuestas para poner remedio a la violación y, si procede, las medidas para mitigar sus efectos

Obligación del RT de documentar cualquier violación de seguridad, los hechos, efectos y medidas correctivas

10.-¿TENGO QUE REALIZAR UNA EVALUACION DE IMPACTO?

Es un proceso para describir los tratamientos, evaluar su necesidad y proporcionalidad, y ayudar a gestionar los riesgos para los derechos y libertades derivados del tratamiento, evaluándolos y determinando las medidas para abordarlos.

El RT debe realizarla cuando sea probable que un tipo de tratamiento entraña un **alto riesgo** para los derechos y libertades.

Las autoridades de control establecerán una lista con los tipos de operaciones de tratamiento que requieran una EIPD.Y podrán elaborar otra lista de las que no lo requieran

10.-¿TENGO QUE REALIZAR UNA EVALUACION DE IMPACTO?

El RGPD establece tres casos en los que es obligatorio la EIPD:

- **Evaluación sistemática y exhaustiva** de aspectos personales de personas físicas que se base en un tratamiento automatizado y **sobre cuya base se tomen decisiones** que produzcan efectos jurídicos para las personas o que les afecten negativamente
- Tratamiento a **gran escala de categorías especiales** de datos
- **Observación sistemática a gran escala de una zona de acceso público.**

10.-¿TENGO QUE REALIZAR UNA EVALUACION DE IMPACTO?

Análisis previo de si hay que realizar o no una EIPD que valore si hay alto riesgo o no.

Criterios de alto riesgo E:\IRUDILAB\CRITERIOS_ALTO RIESGO.pdf

Ejemplos WP248 E:\IRUDILAB\EJEMPLOS EIPD.pdf

E:\IRUDILAB\Guia_EvaluacionesImpacto.pdf

E:\IRUDILAB\GUIA-EVALUACION-DE-IMPACTO-CAT-2.0.pdf

11.- ¿TENGO QUE NOMBRAR UN DELEGADO DE PROTECCION DE DATOS?

Obligación de nombrar un DPO si

- El tratamiento lo realiza una autoridad u organismo público
- Observación habitual y sistemática de interesados a gran escala
- Tratamientos a gran escala de categorías especiales de datos

Posibilidad de nombrar DPO de forma voluntaria.

Supuestos del PLOPD E:\IRUDILAB\DPO EN PLOPD.pdf

11.- ¿TENGO QUE NOMBRAR UN DELEGADO DE PROTECCION DE DATOS?

Designación atendiendo a sus cualidades profesionales y a sus conocimientos especializados del derecho y la práctica en materia de protección de datos.

Debe participar de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos.

Respaldar al RT facilitando los recursos necesarios para sus funciones y el mantenimiento de conocimientos especializados

Independencia en el desempeño de sus funciones.

11.- ¿TENGO QUE NOMBRAR UN DELEGADO DE PROTECCION DE DATOS?

Podrá desempeñar otras funciones y cometidos pero no puede haber conflicto de intereses (no otro cargo que pueda determinar los fines y medios de tratamiento).

No será destituido ni sancionado por desempeñar sus funciones y rendirá cuentas al más alto nivel jerárquico del RT.

Funciones:

- Informar y asesorar al RT o al ET y a los empleados de las obligaciones que les incumben en virtud del RGPD y otras disposiciones de PD.

11.- ¿TENGO QUE NOMBRAR UN DELEGADO DE PROTECCION DE DATOS?

- Supervisar el cumplimiento del RGPD y otras disposiciones de PD y de las políticas del RT o ET en materia de PD

- Asesorar al RT acerca de la EIPD

- Cooperar con la autoridad de control (AGPD).

- Actuar como punto de contacto con los interesados y la AGPD.

E:\IRUDILAB\ASESORAMIENTO Y SUPERVISION DPO.pdf

12.- ¿ESTOY HACIENDO UNA TRANSFERENCIA INTERNACIONAL DE DATOS?

Es transmitir datos fuera del territorio de la **Espacio Económico Europeo** a consecuencia de una cesión de datos o a consecuencia de la prestación de algún servicio.

Los 27 países integrantes de la UE, Islandia, Liechtenstein y Noruega.

A otros países sólo si la **Comisión Europea ha decidido que tienen un nivel de protección adecuado** (Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda y EEUU (Escudo de Privacidad).

No necesitan autorización previa ni notificar a la AGPD

12.- ¿ESTOY HACIENDO UNA TRANSFERENCIA INTERNACIONAL DE DATOS?

Si no está en ninguno de los supuestos anteriores, sólo si el país u organización destinataria **hubiera ofrecido garantías adecuadas** y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

Garantías: Normas corporativas vinculantes, cláusulas tipo de protección adoptadas por la Comisión, cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión, códigos de conducta o mecanismo de certificación

12.- ¿ESTOY HACIENDO UNA TRANSFERENCIA INTERNACIONAL DE DATOS?

Excepciones: Fuera de los supuestos anteriores solo se realizará si el interesado ha dado explícitamente su consentimiento tras haber sido informado de los riesgos; es necesaria para la ejecución de un contrato o de medidas precontractuales adoptadas a solicitud del interesado; por razones importantes de interés público, etc. (art.49)

Si no puede ampararse en ningún supuesto anterior, sólo si no es repetitiva, afecta a pocos interesados y es necesaria a los fines de intereses legítimos imperiosos perseguidos por el RT sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el RT evaluó todas las circunstancias concurrentes y ofreció garantías apropiadas. **Informar a la autoridad de control.**