NUEVO REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

VALENTÍN FAURA

BDO

¿QUÉ ES EL REGLAMENTO GENERAL DE DATOS (RGPD)?

- El RGPD es de directa aplicación en todos los países de la UE.
- Es un texto único que busca homogeneizar la normativa sobre protección de datos personales en la Unión.
- Supone un mayor compromiso de las empresas con la protección de datos. Dota de nuevas herramientas, de nuevos instrumentos para garantizar mejor la privacidad, mejorar la gestión de los interesados.
- Lleva consigo un conjunto importante de nuevas obligaciones y responsabilidades para todas las entidades, implica un cambio importante de enfoque.

¿CUÁNDO?

- El RGPD entró en vigor el 25 de Mayo de 2016.
- Las empresas dispondrán de 24 meses para adecuarse a los requerimientos de seguridad y organizativos.
- El reglamento es de aplicación desde el 25 de mayo de 2018.

¿QUÉ DATOS?

- Al tratamiento de datos personales en el contexto de actividades de un establecimiento del responsable/encargado en la Unión Europea, independientemente de que el tratamiento tenga lugar en la Unión o no.

- Al tratamiento de datos personales de interesados que residan en la Unión europea por parte de un responsable/encargado no establecido en la Unión cuando las actividades estén relacionadas la oferta de bienes y servicios o del control de su comportamiento.

REGLAMENTO

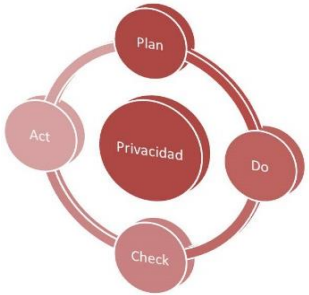
- **Compuesto por 173 disposiciones iniciales, 99 artículos agrupados en 11 capítulos:**

ENFOQUE

- Enfoque basado en los riesgos de privacidad
- Aplicación de controles en base a los riesgos de privacidad
- Toma especial relevancia la diligencia de las Entidades
- Sanciones elevadas: 20 Millones o el 4% facturación anual global

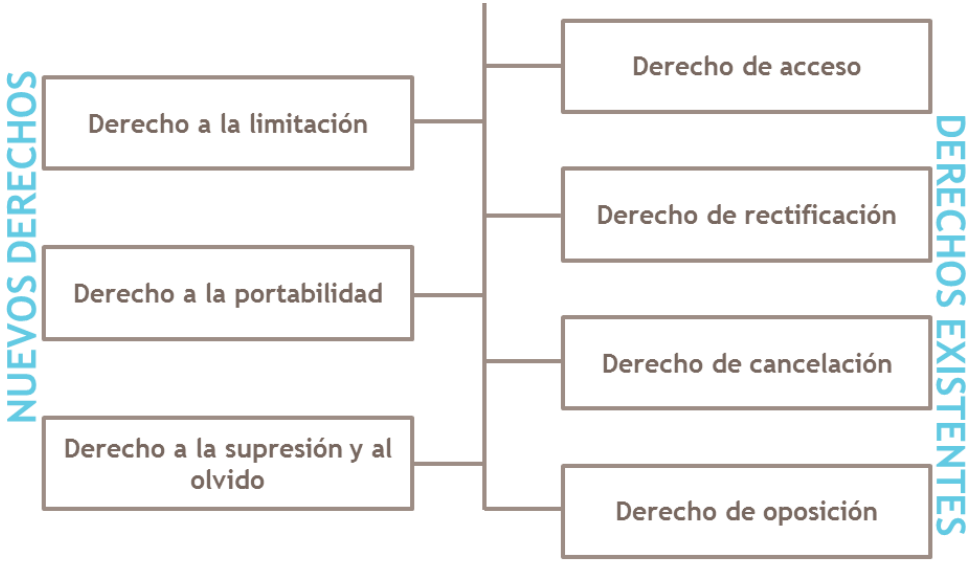
POLÍTICAS, NORMAS Y PROCEDIMINETOS DE PRIVACIDAD

- Aprobación y divulgación de la Política de Privacidad
- Aprobación y divulgación de Normativas y Procedimientos de Privacidad
- Asignación de roles y responsabilidades
- Establecimiento de un Sistema de Gestión de Protección de Datos Personales



PROCEDIMINETOS DE PRIVACIDAD

- Cumplimiento de los derechos de los titulares (ARCO-POL) (30d)



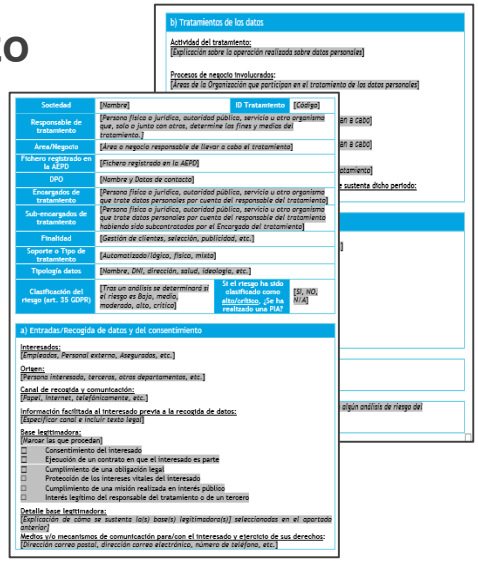
- Clausulados: Clientes, Empleados y Proveedores

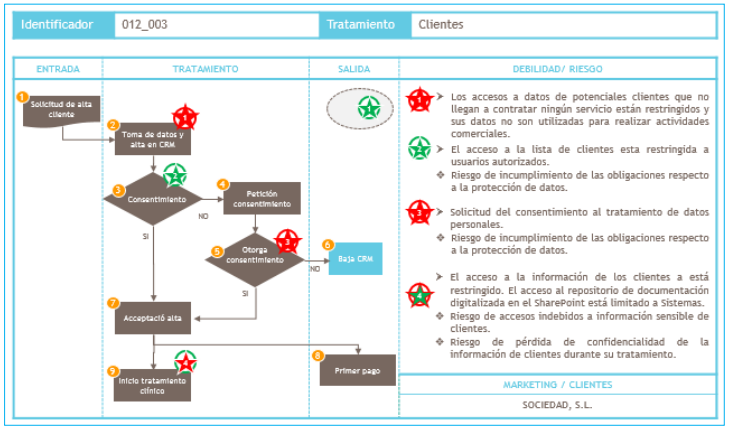
PROCEDIMIENTOS DE PRIVACIDAD

- Gestión y notificación de violaciones de seguridad (72h)
- Protección desde diseño y por defecto
- Gestión de encargados de tratamiento
- Realización de transferencias internacionales de datos personales
- Comunicación interna y externa

REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO (RAT)

- Ciclo de vida de los tratamientos de datos personales:
  - Entrada
  - Tratamiento
  - Salida



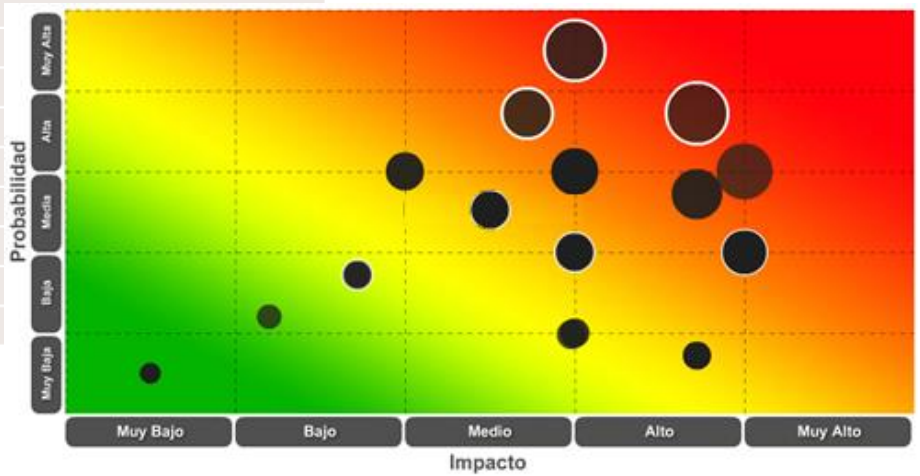


Consentimiento / Base Legitimadora

ANÁLISIS DE RIESGOS DE PRIVACIDAD DE LOS AFECTADOS

No Sensible / Sensible

ID	RIESGOS
R.01	Generales derivados del tratamiento
R.02	Legitimación de los tratamientos y cesiones de datos personales
R.03	Transferencias internacionales
R.04	Notificación de los tratamientos
R.05	Transparencia de los tratamientos
R.06	Calidad de los datos
R.07	Datos especialmente protegidos
R.08	Deber de secreto
R.09	Tratamientos por encargo
R.10	Derechos de los interesados
R.11	Seguridad



EVALUACIONES DE IMPACTO (PIA)

Controles / Riesgo Residual

BDO

Ir a Menú Principal

Inventario de riesgos del tratamiento

Nombre del riesgo	Descripción del riesgo	Aplicabilidad
Ilegitimidad de los tratamientos	• Tratar datos personales no necesarios para la finalidad perseguida • Demasiados datos personales se recopilan respecto al propósito especificado • Carecer de una legitimación clara y suficiente para el tratamiento • Obtener un consentimiento dudoso o inválido • Dificultar la revocación del consentimiento u oposición al tratamiento o cesión • No se puede garantizar la legitimidad de la recogida y la cesión de datos provenientes de terceros • Enriquecer los datos personales de forma no prevista en las finalidades iniciales. • Reidentificación de datos anonimizados que permiten singularizar una persona, inferir información relativa a esa persona o vincular registros relativos a dicha persona.	No
Transferencia Internacional	• Carencia de mecanismos de control de cumplimiento para la transferencia • Impedimentos por parte del receptor para los procedimientos de supervisión y control • Incapacidad de ajudar al afectado en el ejercicio de sus derechos ante el tercero • No obtención de las autorizaciones legales necesarias	No
Transparencia de los tratamientos	• No informar al afectado sobre el por qué y cómo se recogen sus Datos Personales. • Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada • Ubicar la información para el afectado en materia de protección de datos en lugares de difícil localización • Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida el entendimiento de los afectados	No
Calidad de los Datos	• Garantías insuficientes para el uso de datos con fines históricos, científicos o estadísticos. • Realizar inferencias o deducciones erróneas (y, en su caso, perjudiciales) mediante la utilización de técnicas de inteligencia artificial, reconocimiento facial o análisis biométricos.	No
Riesgos asociados a encargados de tratamiento	• Violación de los requisitos legales y regulatorios en los contratos con encargados de tratamiento. • Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas. • Dificultades para comprobar que el encargado y los subcontratistas cumplen las medidas de seguridad • Deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos realizados ante los encargados de tratamiento • Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez	No
Derechos del usuario	• Dificultar o imposibilitar el ejercicio de los derechos del afectado. • Las peticiones de ejercicio de derechos no se gestionan de manera oportuna. • Carencia de procedimientos y herramientas para la gestión de los derechos del afectado. • Carencia de procedimientos y herramientas para la comunicación de derechos	No
Seguridad y deber de secreto	• Deficiencias organizativas en la gestión del control de accesos • Deficiencias técnicas en el control de accesos que permitan acceso no autorizados • Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo • Deficiencias en la protección de la confidencialidad de la información • Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados • Inadecuado procedimiento de gestión de incidentes de seguridad • Controles de acceso a datos inapropiados o deficiente que crean una exposición a la pérdida de datos personales • Falta de concienciación sobre privacidad de datos	Leve
Incorrecta retención de datos	• Los Datos Personales son retenidos inapropiadamente (acumulación innecesaria de datos personales.) • Los datos personales no están correctamente protegidos contra la perdida, destrucción, falsificación o acceso no autorizado. • Carecer de procedimientos claros y de herramientas adecuadas para garantizar la cancelación de oficio de los datos personales una vez que han dejado de ser necesarios para la finalidad o finalidades para las que se recogieron.	No

Actualizar

BDO

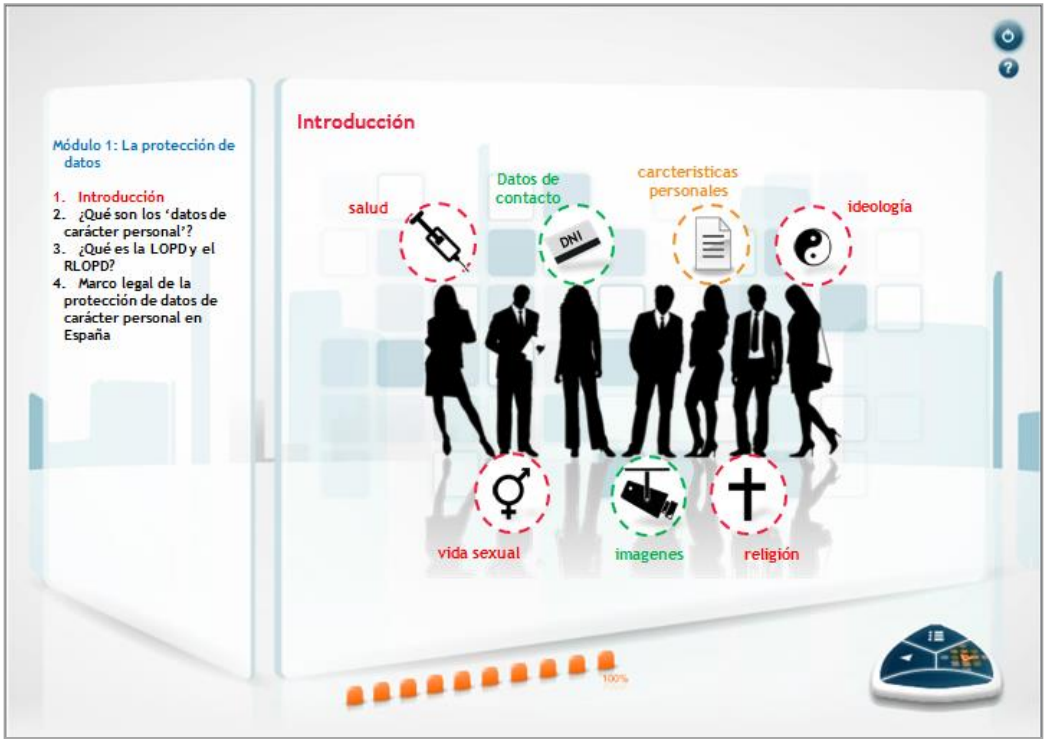
Ir a Menú Principal

Controles a aplicar al tratamiento

Nombre del ries	Descripción del riesgo	Control	Descripcion Control	Impacto tras implementación de los controles	Probabilidad tras implementac	Fiesgo Residual
Seguridad y deber de secreto	• Deficiencias organizativas en la gestión del control de accesos • Deficiencias técnicas en el control de accesos que permitan acceso no autorizados • Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo • Deficiencias en la protección de la confidencialidad de la información • Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados • Inadecuado procedimiento de gestión de incidentes de seguridad • Controles de acceso a datos inapropiados o deficiente que crean una exposición a la pérdida de datos personales • Falta de concienciación sobre privacidad de datos	Control 33	La organización dispone de Políticas, Normas, Procedimientos de seguridad así como de procesos de autorización.			
Seguridad y deber de secreto	• Deficiencias organizativas en la gestión del control de accesos • Deficiencias técnicas en el control de accesos que permitan acceso no autorizados • Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo • Deficiencias en la protección de la confidencialidad de la información • Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados • Inadecuado procedimiento de gestión de incidentes de seguridad • Controles de acceso a datos inapropiados o deficiente que crean una exposición a la pérdida de datos personales • Falta de concienciación sobre privacidad de datos	Control 34	La organización dispone, gestiona y monitoriza la seguridad de la información en base a un análisis de riesgos.			
Seguridad y deber de secreto	• Deficiencias organizativas en la gestión del control de accesos • Deficiencias técnicas en el control de accesos que permitan acceso no autorizados • Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo • Deficiencias en la protección de la confidencialidad de la información • Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados • Inadecuado procedimiento de gestión de incidentes de seguridad • Controles de acceso a datos inapropiados o deficiente que crean una exposición a la pérdida de datos personales • Falta de concienciación sobre privacidad de datos	Control 35	Se identifica y documenta la arquitectura de seguridad del sistema de información.			

BDO

CONCIENCIACIÓN Y FORMACIÓN EN PRIVACIDAD



ACCOUNTABILITY

- Inventario de métricas
- Seguimiento y medición
- Revisión del Sistema de Gestión de Privacidad
- Auditorías del RGPD

¿CÓMO LES PODEMOS AYUDAR?

Entidades / Colectivos

➢ Oficina de soporte al DPO

Supervisión

Se supervisará de forma permanente el cumplimiento de los requisitos de la legislación, entre ellos los asociados a los tratamientos existentes y a la puesta en marcha de nuevos tratamientos.

Asesoramiento

Se prestará un servicio de asesoramiento tanto reactivo (resolución de consultas y peticiones bajo demanda) como proactivo (asesorar sobre novedades de interés en el campo de la privacidad).

Comunicación

Se ofrecerá a la Entidad un servicio de relación y comunicación que combina las reuniones presenciales, comunicaciones vía telefónica y vía email con teléfono y buzón dedicado, con el objetivo de ofrecer un completo y rápido servicio.

¿CÓMO LES PODEMOS AYUDAR?

Entidades / Colectivos

➢ Auditoría de la Adecuación al RGPD de la Entidad

POLITICA Y NORMAS DE PRIVACIDAD	▪ Revisión de la Política, Normas y Procedimientos ▪ Revisión del Sistema de Gestión de la Privacidad
REVISIÓN DEL INVENTARIO Y FLUJOS DE DATOS	▪ Revisión del registro de tratamiento de datos, las medidas de seguridad para asegurar la privacidad de los datos y la actualización contractual con proveedores.
EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS	▪ Revisión del modelo de análisis de riesgos de privacidad y la Realización de una evaluación de impacto siempre que el tratamiento suponga un elevado riesgo para la protección de datos personales de los interesados.
REVISIÓN MEDIDAS TECNICAS	▪ Revisión de las medias establecidas respecto al Art 32 del RGPD y el cumplimiento con los requerimientos de protección de datos desde el diseño y por defecto.
DERECHOS	▪ Derechos ARCO y nuevos derechos de supresión, limitación y portabilidad. Incluye los protocolos para la notificación, registro, ejecución y respuesta a derechos.
CONSENTIMIENTO	▪ Requerimientos relativos a la evaluación de la legitimidad de tratamiento y obtención de consentimientos de los interesados.

Valentín Faura
valentin.faura@bdo.es

bdo.es
bdo.global