EXCMA. DIPUTACIÓN PROVINCIAL DE BURGOS

OBLIGACIONES DEL RESPONSABLE (RT) Y ENCARGADO DEL TRATAMIENTO (ET) RGPD (UE) 2016/679 (27.04.2016)

APLICABLE: 25 MAYO 2018

Cristina Bonal Fdez. Abogado. Derecho NT/PD. cbf@lifeabogados.com

lifeabogados.com

Esquema

1. Unos datos sobre los datos. Nuevo paradigma RGPD
2.- Que supondrá la aplicación del RGPD
3.- Obligaciones RT, ET
   - ✓ Obligaciones generales:
     - Responsabilidad RT
     - Protección desde el diseño y por defecto
     - Co-responsables
     - Designación Representantes en UE
     - Encargado tratamiento (garantías)
     - Registro de actividades
     - Tratamiento bajo autoridad del RT / ET
     - Cooperación con AC
   - ✓ Obligaciones en relación a la seguridad de los datos
   - ✓ Atención derechos interesados
4.- Actuaciones. Pasos a seguir
5.- Textos y normativa

1 UNOS DATOS SOBRE LOS DATOS

- Cada dos días se crea más información que la generada hasta 2003
- El 90% de los datos en el mundo se crearon en los últimos dos años
- Cada minuto se envían 204 millones de emails, 1,8 millones de Facebook Likes, 278.000 twits, 200.000 fotos en Facebook
- Google procesa 40.000 búsquedas por segundo
- Se almacenan 100 horas de vídeos nuevos por minuto en YouTube
- Se crean 570 nuevos web sites por día
- Los centros de datos ocupan una superficie de 6.000 Hectáreas
- Más de 1.200 millones de smart phones en el mundo

Evolución del sustrato material de la privacidad

Analógico	Ficheros de papel, formularios, candados, seguridad física
Digital	Ficheros electrónicos, bases de datos, medios de almacenamiento,
Internet	Páginas web, redes sociales, inter-conexión
IoT	sensores, analíticas big data, hyper-conexión a nivel mundial de cualquier objeto

En clave de humor...

2 ¿QUÉ SUPONDRÁ LA APLICACIÓN DEL RGPD?

NUEVO PARADIGMA RGPD

INCLUIR LA PRIVACIDAD EN LA TOMA DE DECISIONES DE LAS EMPRESAS Y ORGANIZACIONES (AAPP)

ACCOUNTABILITY

El Reglamento intensifica la responsabilidad y la obligación de rendir cuentas de todos aquellos que procesen datos personales (RT, ET)


¿Plazo...? DOS AÑOS PARA ...
DOCUMENTACIÓN Y REGISTRO OBLIGATORIO DE TRATAMIENTOS
COMUNICACIÓN A USUARIOS Y A AUTORIDADES DE CONTROL DE BRECHAS DE SEGURIDAD
REVISIÓN MEDIDAS SEGURIDAD ENS)
ANÁLISIS PREVIO DE TRATAMIENTOS QUE REPRESENTEN RIESGOS PARA LA PRIVACIDAD (EIPD)
ATENCIÓN DE NUEVOS DERECHOS DE LOS INTERESADOS (TRANSPARENCIA, INFORMACIÓN, LIMITACIÓN, PORTABILIDAD)
¿Qué tratamientos lleva a cabo mi Corporación?
Gestión brechas de seguridad
Enfoque según el riesgo
Evaluar los riesgos de un nuevo tratamiento
¿Cómo afectará el RGPD a la relación con los administrados?
PLAN DE FORMACIÓN Y CONCIENCIACIÓN
ELECCIÓN ENCARGADOS TRATAMIENTO
DESIGNACIÓN DPD

3 OBLIGACIONES RT/ET (se han incrementado)

RT (responsable tratamiento): Responsabildiad proactiva

Accountability → **demostrar cumplimiento/carga prueba**

deber de diligencia

Documentación. Registro de actividades
Privacidad por defecto y privacidad desde el diseño.
Seguridad y análisis de riesgos (PIA).
Los códigos de conducta
Diligencia en nombrar proveedores
Notificación violaciones seguridad

ET (encargados del tratamiento) "Encargado seguro": ofrecer garantías suficientes

Los encargados del tratamiento tienen obligaciones expresas y responsabilidades mayores que en el anterior marco regulatorio (registro de actividades de tratamiento, medidas de seguridad , DPD, subcontratación)

Cambia el concepto de encargado del tratamiento, hacia un **"encargado seguro"** de forma que el contrato que regula la relación de estos prestadores de servicios se refuerza, exigiendo que quede todo estipulado (obligaciones).

OBLIGACIONES GENERALES Arts. 24-31 + Considerandos 13, 39, 74-83

RT	ET
RESPONSABILIDAD PROACTIVA. **ART. 24** MEDIAS TÉCNICAS ORGANIZATIVAS APROPIADAS + CUMPLIR RGPD + DEMOSTRAR CÓDIGO CONDUCTA MECANISMO CERTIFICACIONES **OBLIGACIÓN GENERAL DE DILIGENCIA EN SELECCIÓN DE ENCARGADO** →	**ART. 28 OFREZCA GARANTÍAS SUFICIENTES** (APLICAR MEDIDAS TECN. Y ORGANIZ. + ADOPCIÓN MEDIDAS) CONTRATO- ACTO JURÍDICO (oblgs. del ET), contenido mínimo: -tratar DPs siguiendo instrucciones documentadas del RT (salvo exigencia legal del ET bajo ley UE/EE.MM. de la que tiene que informar el ET). -garantizar que el personal autorizado está sujeto a confidencialidad -adoptar las medidas de seguridad del RGPD -SUBCONTRATACIÓN: (i) autorización previa escrita, específica o general del RT; (ii) mismas oblgs. por contrato; (iii) resp. por incumplimiento del subcontratista -asistir al RT respecto de solicitudes de dº, oblgs. seguridad, notificaciones violaciones, DPIA y consulta previa -a elección del RT: suprimir o devolver DPs al terminar la prestación de servicios y suprimir copias existentes salvo conservación impuesta por ley UE/EE.MM. -poner a disp. del RT info. necesaria para demostrar cumplimiento de estas oblgs. -permitir auditorías, inspecciones por RT **ADHESIÓN COD CONDUCTA/CERTIFICACIONES** (demostrar garantías suficientes) FIJAR CLAUSULAS CONTRACTUALES TIPO POR AC/COMISION EU ART. 28.10 RESPONSABILIDAD EN CASO INCUMPLIMIENTO RGPD AL DETERMINAR FINES-MEDIOS TRATAMIENTO (RT)

RT	ET
CORRESPONSABLES TRATAMIENTO. ART. 26 DEFINEN CONJUNTAMENTE objetivos y medios Tto ACUERDO: determinar responsabilidades respectivas, a disposición interesados EJERCICIO DERECHOS POR LOS INTERESADOS frente y en contra de cada RT	---------
DESIGNAR REPRESENTANTE EN UE . ART. 27 RT/ET NO ESTABLECIDOS EN UE, A INTERESADOS DE LA UE EXCEPCIONES (AUTORIDADES ORGANISMOS PÚBLICOS, TTO OCASIONAL/NO CATEG. ESPECIALES DATOS, IMPROBABLE RIESGO) ESTABLECIDO EN ESTADO DONDE ESTÉN INTERESADOS ATENCIÓN (junto con RT Y ET) CONSULTAS DE AC/INTERESADOS SI PERJUICIO ACCIONES FRENTE A RT/ET	IDEM
COOPERACIÓN CON AUTORIDAD DE CONTROL (AC/AGPD) ART. 31 RT/REPRESENTANTES	IDEM

RT	ET
REGISTRO DE ACTIVIDADES DE TRATAMIENTO ART. 30 POR ESCRITO/FORMATO ELECTRÓNICO + A DISPOSICIÓN AC (EQUIVALENTE DOC SEGURIDAD ACTUAL) > 250 TRABAJADORES <250: RIESGO NO SEA OCASIONAL, INCLUYA CATEGORÍAS ESPECIALES DATOS, DATOS DE CONDENAS/INFRACCIONES PENALES ART. 30.1 CONTENIDO - DATOS RT, RTTE, DPO - FINES - CATEGORÍAS INTERESADOS, Y DATOS PERSONALES - CATEGORÍAS DESTINATARIOS - TRANSFERENCIAS INTERNAC Y GARANTÍAS - CUANDO SEA POSIBLE: PLAZO SUPRESIÓN DATOS, DESCRIPCIÓN GRAL MEDIDAS	IDEM A DISPOSICIÓN AC ART. 30.2 CONTENIDO - DATOS RT, RETTE, DPO - CATEGORÍAS TTOS POR CUENTA RT - TRANSFERENCIAS INTERNAC. Y GARANTÍAS - DESCRIPCIÓN GRAL MEDIDAS
DESIGNAR DPD ART. 37 a 39 OBLIGATORIO: AUTORIDAD U ORGANISMO PUBLICO PLANTILLA/CONTRATO SERVICIOS	IDEM

RT	OBLIGACIONES EN RELACIÓN A LA SEGURIDAD DE LOS DATOS	ET
ADOPCIÓN MEDIDAS TÉCNICAS Y ORGANIZATIVAS APROPIADAS, RESULTADO DEL ANÁLISIS DE RIESGO Y DE LAS EVALUACIONES DE IMPACTO (NO MEDIDAS PREDEFINIDAS). ART. 32 + CONS. 74-77, 83. ENS, ISO 27001Factores: estado de la técnica; costes de aplicación; naturaleza, alcance, contexto y fines del tratamiento; probabilidad y gravedad del riesgo para dº y libs. (en particular, como consecuencia destrucción, pérdida o alteración accidental o ilícita de DPs o comunicación/acceso no autorizados): - Cifrado, seudonimización (ACLARACIÓN: reducción de riesgos. El dato seudonimizado está sometido al Reglamento - Confidencialidad, integridad disponibilidad, resilencia - Incidente físico-técnico: capacidad restaurar disponibilidad - Verificación, evaluación, valoración regulares de la eficacia medidas ADHESIÓN CÓDIGOS CONDUCTA/CERTIFICACIÓN RT/ET MEDIDAS QUE GARANTICEN QUE QUIEN ACTÚE BAJO SU AUTORIDAD Y ACCEDA A DPs SIGA INSTRUCCIONES RT . **ART 29**		IDEM
VIOLACIÓN SEGURIDAD PD (salvo no riesgo DLP) **ART. 33,34** 1. Notificación a AC, Art. 33 salvo no probabilidad riesgo - Sin dilación indebida/**max. 72 horas** (más tiempo: motivos) - Requisitos notificación simultanea/gradual (naturaleza (inclusive, si es posible, categorías y nº aprox. de interesados y DPs afectados), dato/contacto DPD, posibles consecuencias, medias adoptadas/propuestas para remediar/mitigar efectos) - Documentar violaciones seguridad (a disposición AC) 2. AL INTERESADO ART. 34: alto riesgo DLP (sin dilación indebida, lenguaje claro, sencillo). Excepciones (cifrado, medidas, esfuerzo desproporcionado –comunicación pública-) AC puede obligar a notificar a interesados	←	NOTIFICAR AL RT Sin dilación indebida

RT	ET
EVALUACIÓN DE IMPACTO PD (EIPD) ART. 35 + CONS. 75, 84, 89-93 **QUE ES?** análisis de los riesgos que un producto o servicio puede entrañar para la protección de datos de los afectados y, como consecuencia de ese análisis, la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos. ANALISIS TTOS, NATURALEZA, ALCANCE, CONTEXTO, FINES: **CUANDO**: ANTES DE INICIAR TTO + ENTRAÑEN **ALTO RIESGO DLP.** **SUPUESTOS**: **GUIA GT29 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_es.pdf** - decisiones basadas en EVALUACIÓN SISTEMÁTICA , EXHAUSTIVA Y AUTOMATIZADA (elaboración de perfiles) de aspectos personales con efectos jurídicos personas o efectos significativos similares -tratamiento a GRAN ESCALA de categorías especiales datos + condenas infracciones penales - OBSERVACIÓN SISTEMÁTICA a gran escala de zona de acceso público * Exista un cambio del riesgo que representen las operaciones de tratamiento NO APLICA: -tratamiento basado en deber legal o interés público bajo ley UE/EE.MM. que lo regule específicamente -PIA ya realizado como parte de una evaluación de impacto general en el contexto de la adopción de la ley (salvo que EE.MM. regule lo contrario) **-AC podrá establecer LISTAS OPERACIONES TTO SI/NO.** **ALCANCE** : - Descripción sistemática de: (i) operaciones de tratamiento y (ii) finalidad - Evaluación de: (i) la necesidad y la proporcionalidad del tratamiento con respecto a su finalidad (ii) los riesgos para los dº y libs ***** El cumplimiento de códigos de conducta por los RT o ET se tendrá en cuenta al evaluar las repercusiones del tratamiento -Medidas previstas para afrontar los riesgos (incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales) **+** "Cuando proceda", Opinión de los interesados o de sus representantes "sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento" RECABAR **ASESORAMIENTO DPO** ÚNICA EVALUACIÓN/PIA CONJUNTA PARA OPERACIONES DE TTO/RIESGOS SIMILARES. Considº 92 (AAPP *aplicación o plataforma común de tratamiento; grupo ayuntos. crean servicio atención remota a mayores, etc.* **¿QUIÉN, CÓMO**? INTERNA-EXTERNA + USO METODOLOGÍAS ADECUADAS (MAGERIT, Guia Gestión de Riesgos INCIBE, AGPD) ttps://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf)	---

Riesgo alto para dchos y libertades personas GT29:

- Evaluación o *scoring,* incluida la elaboración de perfiles o *profiling*, especialmente en relación con aspectos relacionados con el rendimiento laboral, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado. Como ejemplo, *supuesto de una empresa de biotecnología que ofrece pruebas genéticas directamente a los consumidores con la finalidad de predecir una enfermedad o riesgo para la salud.*
- Observación sistemática a gran escala de una "zona de acceso público", que deberá interpretarse según el GT29 como cualquier lugar abierto al público (*por ejemplo, una plaza, un centro comercial, una calle o una biblioteca pública*).
- Tratamiento de datos a "gran escala", que deberá interpretarse según el GT29 teniendo en cuenta los siguientes criterios: *el número de afectados, el volumen de los datos, la duración o permanencia del tratamiento de datos y, por último, la extensión geográfica en la que se vaya a llevar a cabo el tratamiento de datos.*
- Datos relativos a "personas vulnerables". Dentro de tal denominación, el GT29 considera como personas vulnerables a *empleados (en lo relativo a la gestión de recursos humanos), niños, enfermos mentales, solicitantes de asilo, ancianos y pacientes, así como cualquier otro supuesto en el que se pueda dar un desequilibrio entre la posición del interesado y el responsable del tratamiento.*
- El uso de soluciones tecnológicas innovadoras (por ejemplo, *la combinación del uso de la huella dactilar y el reconocimiento facial a fin de mejorar el control de acceso físico a unas instalaciones).*
- Transferencias de datos fuera de la Unión Europea.

Tto a gran escala

Número de afectados
Volumen y rango de los datos
Duración de la actividad
Extensión geográfica

Recomendaciones

El GT29 considera que cuantos más criterios se cumplan, más probable será que el tratamiento de datos se considere de alto riesgo para los derechos y libertades de los interesados y, por tanto, se deba exigir la realización de una EIPD.

A este efecto, el GT29 considera como regla, que el cumplimiento **de dos o más** de los criterios mencionados conllevará la obligación de realizar la EIPD.

Si el Responsable, aún cumpliendo dos o más de los criterios considera que no existe un alto riesgo tendría que documentar de forma exhaustiva las razones para no llevar a cabo la EIPD.

Periodicidad EIPD: cada **3 años**

RT	ET
CONSULTA PREVIA AC , ART. 36 + CONS. 94-96: (ALTO RIESGO NO MITIGABLE. GT29 "**alto riesgo residual**". **-** POR ESCRITO -FACILITAR INFORMACIÓN: -Responsabilidades del RT, Co-RT, ET (en particular, tratamientos intra-grupo empresarial); -Fines y medios de tratamiento; -Medidas y garantías para proteger DYL -Datos de contacto DPO *Otra información que solicite la AC* -PLAZOS: - 8 semanas + 6 semanas si es complejo - 1 mes para informar RT/ET (extensión prórroga y motivos) -Uso por AC poderes Art. 58 GDPR (investigación, corrección, autorización y asesoramiento) -CONSULTA PREVIA de los EEMM (ESTADOS MIEMBROS) a AC (AGPD) en la preparación de una PROPUESTA LEGISLATIVA a adoptar por Parlamento nacional o medida regulatoria derivada, que se refiera a un tratamiento de datos personales.	--------

FACILITAR DERECHOS DEL INTERESADO ARTS 13 y ss.	
TRANSPARENCIA DE LA INFORMACIÓN: CONCISA, TRANSPARENTE, INTELIGIBLE, y de FÁCIL ACCESO	Colaboración con RT
Derechos : ACCESO, RECTIFICACIÓN Y SUPRESIÓN (OLVIDO), LIMITACIÓN TRATAMIENTO, PORTABILIDAD, OPOSICIÓN Y DECISIONES INDIVIDUALES AUTOMATIZADAS (elaboración perfiles) COMUNICACIÓN BRECHA SEGURIDAD	Incluir en contrato (servicios)

4

Queda UN AÑO … PASOS A SEGUIR

https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Impacto_RGPD_en_AAPP.pdf

REGISTRO DE ACTIVIDADES DE TTO
(Ficheros notificados - documento seguridad)
Datos RT, DPD, Fines, Usos, plazo conservación, etc

¿Conozco todos los tratamientos que lleva a cabo mi organización?

IDENTIFICAR FINALIDADES Y BASE JURÍDICA TRATAMIENTOS
Consentimiento
Interés legitimo
obligación legal
Contrato
Satisfacer interés publico
Ejercicio poderes públicos
(establecido en norma de rango legal)

¿Son lícitos los tratamientos?
¿Datos necesarios?

REVISIÓN/ADECUACIÓN CLÁUSULAS: INFORMATIVAS CONSENTIMIENTO
("Categorías especiales de datos": servicios asistencia social, salud pública, prevención, menores)

¿Estoy preparado para evaluar los riesgos de un nuevo tratamiento?

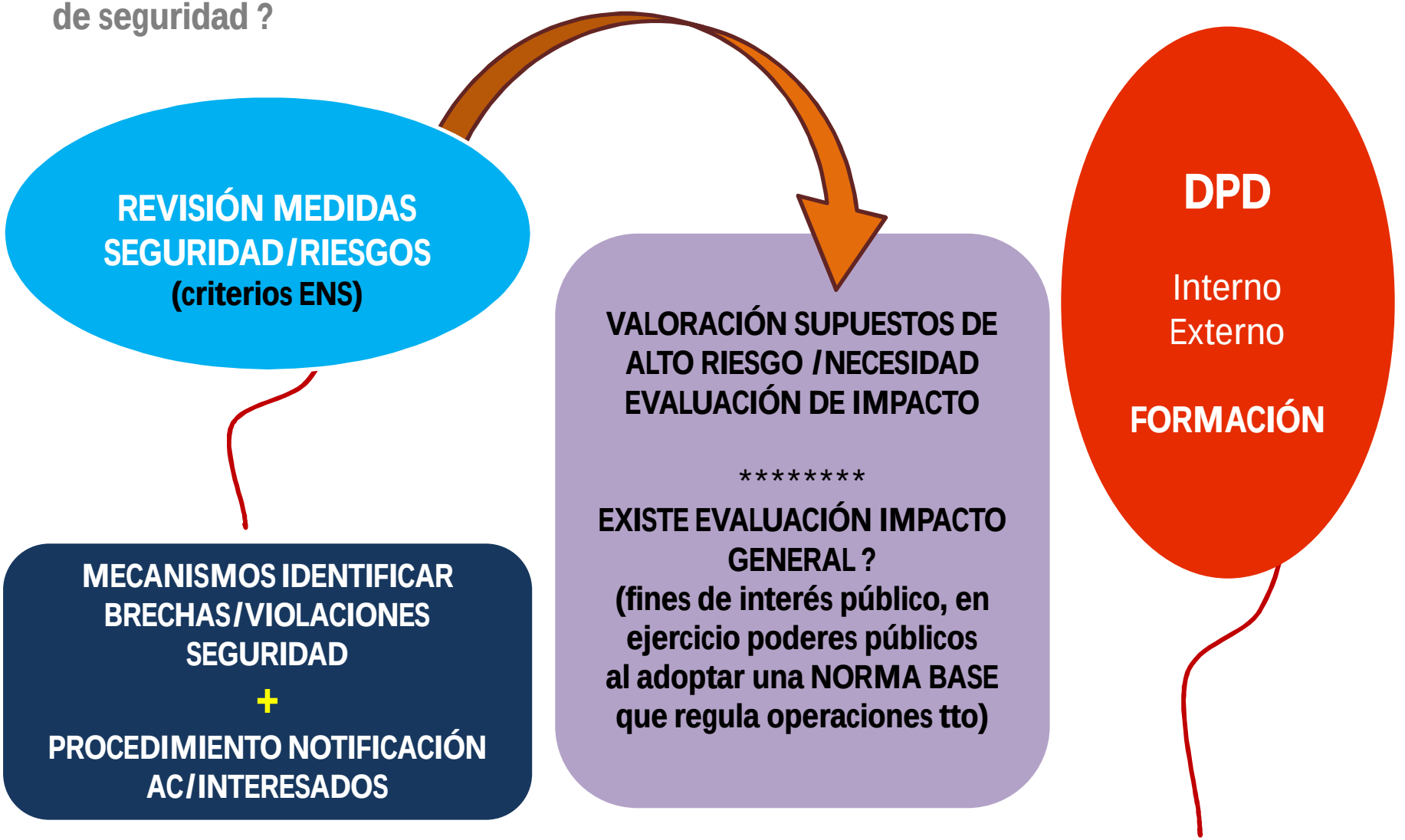
EJERCICIO DERECHOS DE LOS INTERESADOS: MECANISMOS VISIBLES, SENCILLOS, ACCESIBLES (+ ELECTRÓNICOS) (ESPECIAL ATENCIÓN NUEVOS DERECHOS)

¿Cómo afectará el RGPD a la relación con los administrados?

CONTRATOS ET
ADECUACIÓN/REVISIÓN, CONVENIOS AAPP, SUBCONTRATACIÓN! FIJACIÓN FUNCIONES, RESPONSABILDIADES

Diligencia en la elección ET

¿Son adecuadas al nivel de riesgo las medidas de seguridad actualmente existentes? ¿debo hacer una Evaluación de Impacto? ¿Cómo debo actuar si se produce una brecha de seguridad ?



AAPP: autoridad, organismo público, empresa que presta servicios públicos


CREACIÓN DE
UNA ESTRUCTURA DE
CUMPLIMIENTO INTERNO
Y ASIGNACIÓN DE
RESPONSABILIDADES
+
FORMACIÓN Y CONCIENCIACIÓN
CULTURA DE LA PRIVACIDAD

5 Textos, normativa

- **Carta de los Derechos Fundamentales de la Unión Europea** Art. 8, 1: toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
- **Constitución Española**, Art. 18.4 : 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
- **SENTENCIA TC 292/2000, DE 30 DE NOVIEMBRE (HABEAS DATA)**: derecho fundamental a la autodeterminación informativa, en virtud del cual, debe ser el interesado el que decida QUIÉN puede tener sus datos y PARA QUÉ se usan. Para que este derecho sea efectivo es necesario que el ciudadano sea INFORMADO PREVIAMENTE, al objeto de que pueda ejercer su derecho de opción.
- **Ley 15/1999 Ley Orgánica 15/1999, de 13 de diciembre**, de Protección de Datos de Carácter Personal LOPD (hasta 25 mayo 2018)
- **Real Decreto 1720/2007, de 21 de diciembre**, por el que se aprueba el Reglamento de desarrollo de la LOPD (hasta 25 mayo 2018)
- **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

- **RD 3/2010 Real Decreto 3/2010, de 8 de enero**, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- **Ley 19/2013, de 9 de diciembre, de transparencia**, acceso a la información pública y buen gobierno.
- **Ley 39/2015, de 1 de octubre**, del Procedimiento Administrativo Común de las Administraciones Públicas.
- **Ley 40/2015, de 1 de octubre,** de Régimen Jurídico del Sector Público.

  Ambas disposiciones, vienen a configurar un escenario en el que la tramitación electrónica debe constituir la actuación habitual de las Administraciones en sus múltiples vertientes de gestión interna, de relación con los ciudadanos y de relación de AAPP entre sí.
- **Ley 7/1985** Reguladora de las Bases de Régimen Local
- **RD Legislativo 3/2011 de 14 de noviembre**, por el que se aprueba el Texto Refundido de la Ley de Contratos del Sector Público
- **Real Decreto Legislativo 2/2004, de 5 de marzo**, por el que se aprueba el texto refundido de la Ley Reguladora de las Haciendas Locales
- **Ley 58/2003, de 17 de diciembre**, General Tributaria.
- **AGPD y GT29:** GUÍAS ORIENTACIONES DIRECTRICES: http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php
- Disposición adicional segunda Ley 39/2015: **'Adhesión de las Comunidades Autónomas y Entidades Locales a las plataformas y registros de la Administración General del Estado'** https://administracionelectronica.gob.es/pae_Home.html#.WUpJVuvygdU
- **Diputación Provincial Burgos**: http://www.burgos.es/

Muchas gracias

Cristina Bonal Fdez. Abogado. Derecho NT/PD. cbf@lifeabogados.com

lifeabogados.com