Anexo nº 2

Cuadro remitido al Consejo de Estado 4/8/2017

SUBSECRETARÍA

SECRETARÍA GENERAL TÉCNICA

SUBDIRECCIÓN GENERAL DE POLITICA LEGISLATIVA

ASOCIACIÓN/EMPRESA	SUGERENCIAS
ISACA MADRID	Mejor derogar que modificar la normativa española vigente y actuar de forma coordinada con el resto de países en la redacción de una normativa nacional sustitutoria
UNESPA	-Con el nuevo Reglamento comunitario, al no tener en cuenta las especificidades sectoriales, pueden verse afectados adversamente los tratamientos de datos que se realizan por el sector. -Se analiza el impacto en el sector asegurador de determinadas figuras reguladas en el reglamento: 1. Consentimiento y elaboración de perfiles. 2.Principio de responsabilidad activa. 3. Derecho a la portabilidad de los datos.
TELEFÓNICA	**-Efectividad de los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias: requiere que se** creen los incentivos necesarios para que las empresas y los interesados acudan a ellos. -promover la elaboración de **códigos de conducta** destinados a contribuir a la correcta aplicación de Reglamento. -necesario desarrollar los criterios para que**los administrados conozcan las consecuencias de sus actos en materia de incumplimientos de la normativa** de protección de datos tanto a nivel de la multa como de los tipos de agravantes y atenuantes a los efectos de valorar el nivel de culpabilidad a imputar. En otros cuerpos normativos en los que el legislador europeo ha optado por un modelo de fijación de multas análogo en función del volumen de negocio (Derecho de la Competencia) se han publicado **circulares** que avanzan el criterio o secuencia de análisis a la hora de fijar importantes multas en función del volumen de negocio de las

SAN BERNARDO, 62
28015 MADRID
TEL: 91 390 45 22
FAX: 91 390 22 32

	empresas. **Una opción análoga en nuestro ordenamiento jurídico aportaría esa exigencia de predictibilidad necesario para que toda actuación sancionadora se realice conforme a la Constitución Española.**
GESTORES ADMINISTRATIVOS MADRID	Se debe contemplar la figura del **gestor administrativo colegiado como Delegado de Protección de Datos** (art.37.5 Directiva), tanto por las funciones que ejercen como por las que se reconocen a los Colegios Oficiales de gestores administrativos como órganos de certificación.
ASIPRODAT (Asociación de interesados para la protección de datos)	Es necesario derogar la LOPD y su normativa de desarrollo y regular el tratamiento de datos en ciertos **sectores** (publicidad, datos sensibles,videovigilancia,ámbito laboral,personas fallecidas, menores en todos los ámbitos, investigación, expresión artística de todo tipo)
CECA	1. Observaciones generales: normativa (listado abierto) que deben cumplir las entidades de crédito y que implica tratamientos obligatorios que deberían quedar exentos del cumplimiento de los requisitos normalmente exigibles en materia de protección de datos de carácter personal: -**Prevención del blanqueo de capitales y financiación del terrorismo y cumplimiento de políticas de sanciones internacionales.** - **Normativa tributaria.** respecto del cumplimiento de obligaciones de información relativa a datos fiscales o a cuentas financieras, la legitimación para el tratamiento de los datos estrictamente necesarios para la correcta ejecución de la obligación requerida (en virtud de una norma, y, también, derivadas de un acuerdo entre España y un tercer país) debería basarse en la obligación legal, y no en el consentimiento del titular del dato. -**Normativa de Crédito Responsable.** La Ley 2/2011, de 4 de marzo, de Economía Sostenible, desarrollada (respecto del contenido del presente apartado) por la Ley 16/2011, de 24 de junio, de Contratos de Crédito al Consumo (transposición de la Directiva 2008/48/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2008 relativa a los contratos de crédito al consumo), señala en su artículo 14, la obligación de evaluar la solvencia del solicitante. Dicha evaluación debe realizarse sobre la "base de una información suficiente obtenida por los medios adecuados a tal fin" (facilitada por el consumidor o bien obtenida por otros medios). Este tratamiento analítico (automatizado en mayor o menor medida) de datos de carácter personal entendemos debería quedar expresamente excluido de la elaboración de perfiles (artículo 22.2.b. RGPD), puesto que la finalidad del mismo es dar cumplimiento a un mecanismo orientado a otorgar al consumidor el grado de protección que se estima necesario en el ámbito del crédito al consumo. -**Seguridad y prevención del fraude.** resulta imprescindible que las entidades financieras optimicen los procesos de anticipación, detección y monitorización de posibles actividades ilícitas, siendo especialmente necesaria una comunicación constante entre todas las entidades de crédito, los reguladores nacionales e internacionales destinada al intercambio permanente de información, con la estricta finalidad de prevención del fraude y seguridad. El análisis y modelado de datos de carácter personal, mediante tecnologías adecuadas, con dicha exclusiva finalidad de control del

	fraude y la seguridad, debe ser objeto de una atención adecuada y significativa en la normativa sectorial (financiera / seguridad de las entidades de crédito). -**Otras normas que recogen obligaciones legales con impacto directo en materia protección de datos de carácter personal:** o Obligaciones de *reporting* regulatorio a los supervisores y autoridades públicas. o Normativa laboral (directorios de empleados, control empresarial y control de accesos por parte de personas físicas (empleados o proveedores) a los sistemas/dispositivos del empleador en virtud de la relación laboral o contractual). o Salud laboral (prevención de riesgos laborales y salud laboral). 2.Observaciones específicas -**Aclaración de conceptos jurídicos indeterminados**: responsabilidad del art.5.2 RGPD; licitud del tratamiento para fines diferentes sin consentimiento; tratamiento de datos sensibles en el ámbito laboral; datos personales que el interesado ha hecho manifiestamente públicos; confidencialidad de los datos; tratamiento de datos sin necesidad de identificación; fuentes accesibles al público; mercadotecnia directa. - debe otorgarse potestad a la AEPD para la adopción de **cláusulas contractuales tipo** en los contratos que vinculan a responsables y encargados (y, a su vez, sub-encargados) (Art.28.8), y que se establezca el deber de la AEPD de publicar una lista de tratamientos que requieran evaluaciones de impacto (Art. 35.4) y de aquellas que no requieran dichas evaluaciones. Que se establezcan exenciones respecto de la realización de evaluaciones de impacto en el supuesto de tratamientos derivados del cumplimiento de obligaciones legales. -debe precisarse la obligación de consultar a la AEPD en el supuesto de tratamientos realizados por un responsable en el ejercicio de una misión de interés público (art.36) -Se debería detallar cómo deberá ser llevado a cabo el procedimiento de acreditación de organismos certificadores (Art. 43.1). - Se establecen situaciones especificas para poder llevar a cabo transferencias internacionales de datos que no cumplen con los requisitos establecidos, una de ellas, que sea necesaria por razones importantes de interés público (Art. 49 d). El referido interés público debería ser concretado por la norma a proyectar. Deben asimismo definirse las condiciones para la transferencia internacional de datos a un tercer país u organización desde un registro público accesible con carácter general (p.ej. de información obtenida del Registro Mercantil relativa a representantes personas físicas y su eventual transferencia a terceros países).

	-mantener la coherencia del sistema de acción y litigación colectiva, resultaría deseable, para ello, que la acción colectiva se limitase a posibles afectaciones de derechos de consumidores y se limitase la legitimación a aquellasasociaciones que reúnan la condición de "especialmente representativas" La norma específica sobre protección de datos debería contener una mención genérica a la posibilidad de accionar colectivamente que redirigiese a su vez a la LEC y al TRLDCU. - la norma debe prever la imposición de multas administrativas a la Administración (cualquier Administración) por infracción del RGPD (Art. 83.7). **- debería ser concretado lo señalado en el artículo 86, que se refiere a la necesidad de conciliación del acceso del público a documentos oficiales y el derecho a la protección de los datos personales.** **-Es necesario que se establezcan condiciones específicas para el tratamiento del DNI en el ámbito financiero.**
CEOE	**-evaluación de impacto** relativa a la protección de datos: debería existir un **alto grado de flexibilidad**, modelos no obligatorios, o elementos mínimos que se deben incluir en una evaluación de impacto de protección de datos. Se deben considerar **tanto los beneficios como los riesgos** para el sujeto objeto de tratamiento de datos. Es necesario determinar **las características y criterios que son de "alto riesgo** y elaborar una guía general que aborde la metodología de evaluación de riesgos. Se debe encontrar un **equilibrio entre la información que necesitan las autoridades de protección de datos para evaluar los casos individuales y lo que se debe considerar como secreto comercial de una empresa.** **-Ventanilla única y mecanismos de colaboración.** Se ha de reconocer este mecanismo en la legislación española para asegurar un funcionamiento efectivo. -**Redacción propuesta art. 39.3**: en relación a las funciones, obligaciones y responsabilidades del **Delegado de Protección de Datos**, cuando el mismo sea nombrado a pesar de no existir obligación legal para ello, no quedará sujeto a las mismas. Para ello, la posición que ostente esta persona deberá evidenciar claramente que no es un DPD en el sentido propio de la norma. **-Sanciones aplicables al amparo del Reglamento** la implementación interna del Reglamento ha de delimitar, como venía haciendo la LOPD, la graduación de las sanciones, los principios de aplicación por el que se rigen, la prescripción

	de las mismas, etc. reservando, en todo caso, la aplicación de los máximos de las sanciones para los casos más excepcionales y graves evitando convertirlos en recursos cotidianos.
ORANGE ESPAGNE, S.A.U.	-**consentimientos**, expreso e implícito. **Es fundamental que se concreten los supuestos en los que aplica uno u otro consentimiento, así como el alcance y condiciones exigibles en cada caso**. -el Considerando (171) colisiona con el principio de irretroactividad de la ley al **extender la regulación del consentimiento en el Reglamento a hechos pasados, previos a la entrada en vigor del mismo.** Además de resultar contrario a Derecho, conlleva un grave perjuicio económico y operativo para todos los Responsables -**resulta necesaria una aclaración normativa del concepto de interés legítimo**, de su alcance y de los criterios que permitan al responsable acogerse al mismo y, en particular, en los dos supuestos (prevención del fraude y mercadotecnia, en este caso, además, concretando qué se entiende por mercadotecnia y qué tratamientos de datos se englobarían en la misma). -es conveniente que se publiquen, con anterioridad a la entrada en vigor del Reglamento, **guías para la realización de evaluaciones de impacto tanto generales como sectoriales**, con especial referencia a las circunstancias concretas y a los distintos tratamientos de datos que se llevan a cabo en cada sector (telecomunicaciones, financiero, etc.) -**Deben concretarse los casos en los que ha de llevarse a cabo una consulta previa a la autoridad de control, delimitando el concepto de "alto riesgo"** - Mantener una **escala de sanciones** similar a la recogida en el artículo 45 LOPD, en la que se fijan unos importes mínimos y máximos para cada tipo de sanción, garantizando la seguridad jurídica como principio fundamental del Derecho. -Ha de prescindirse de **varios criterios de graduación previstos** en el artículo 45.4 LOPD, como los recogidos en los apartados *c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal* y *d) El volumen de negocio o actividad del infractor***. Ambos criterios penalizan, de por sí, a determinadas entidades, sin atender a las circunstancias concretas de la infracción y al grado de responsabilidad del infractor**.
	Para evitar una situación de incertidumbre en los Responsables y Encargados de tratamientos de datos de carácter

DESPACHO HIGUERA- DESPACHO MARTÍNEZ	personal que actualmente han establecido medidas de seguridad no comparables, por su complejidad, a las de casi ningún otro Estado miembro, entendemos que **las medidas de seguridad que se establezcan en la futura modificación de la Ley Orgánica de Protección de Datos, deberían coincidir en gran medida con las existentes actualmente**, ya que rebajarlas o modificarlas sustancialmente sería perjudicial tanto con la operativa actual de los Responsables y Encargados, puesto que afectaría a la seguridad y tratamiento de esos datos y provocaría una situación de incertidumbre e inseguridad en estos sujetos.
HUAWEI	-La nueva normativa establezca **el acceso eficaz a los datos por parte del titular de los datos personales para no convertir al usuario en un mero titular de una obligación de consentir**. **La transparencia debe ser interpretada como derecho a ser informado de cómo se tratan los datos y a dar un mayor y mejor acceso a los mismos**. -Una aplicación clave para la competitividad de las empresas es que pueda existir, con base en el interés legítimo, **la transferencia internacional y comunitaria de datos de empleados, especialmente dentro de los grupos de empresas.** -la nueva regulación española que sustituya a la actual LOPD debería **recoger el máximo posible de disposiciones sectoriales y de desarrollo**, y debería de adaptarlas aglutinando de esa forma toda regulación existente en materia de Protección de Datos en España, adaptada a la reciente jurisprudencia de los tribunales europeos y en consonancia con la propuesta de Reglamento de e-Privacy.
ASEDIE Asociación Multisectorial de la Información	-aclarar si bajo el Reglamento se mantiene la exclusión del ámbito de aplicación de la legislación de protección de datos del actual art. 2.2. RLOPD, **los datos de contacto de personas físicas en personas jurídicas, ya que , en otro caso,** las empresas infomediarias que actualmente facilitan estos datos obtenidos de las publicaciones del Registro Mercantil, tendrían que llevar a cabo, en cumplimiento del artículo 14 del Reglamento europeo, miles de notificaciones que supondrán un esfuerzo desproporcionado siendo incluso en algunos casos imposible realizarlas. -La posible aplicación de la legislación de protección de datos a los **datos de empresarios individuales y autónomos,** provoca de facto, que queden sujetas a la ley la mayoría de las bases empresariales, ya que éstas incluyen indistintamente entidades jurídicas, autónomos y empresarios individuales, no siendo fácil segmentar las mismas separando una parte de los datos simplemente por la forma jurídica con la que se desarrolla una actividad económica. **Esto podría provocar la exclusión en la prestación de servicios empresariales a autónomos y empresarios individuales**

	-se aclare la base legal bajo la que podrá realizarse el tratamiento de datos de **los ficheros de solvencia patrimonial y crédito** con datos sobre cumplimiento o incumplimiento de obligaciones dinerarias aportados por los acreedores o quienes actúen por su cuenta o interés, actualmente regulados por el art. 29.2 LOPD. Esta base legal no puede ser otra que "el interés legítimo" del art. 6 f) del Reglamento europeo. -**Cambio en los deberes de información al afectado** lleva a la necesidad de modificar todas las cláusulas de información y consentimiento actualmente existentes. Debería, especialmente aclararse, en supuestos como la recogida de datos de nombramientos sociales publicados en el Boletín Oficial del Registro Mercantil, Reglamento).Se debe aclarar también si el momento de la obligación de Información al afectado en la recogida de datos para fines de mercadotecnia mantendrá la consideración actual del artículo 30.2 de la LOPD.De no ser así, las empresas Infomediarias de ASEDIE tendrían que llevar a cabo, en cumplimiento del artículo 14 del Reglamento europeo, miles de notificaciones previas a la realización de la acción publicitaria o prospección comercial, que supondrán sin lugar a dudas un esfuerzo desproporcionado que afectaría gravemente a todo el sector del marketing publicitario, siendo incluso en algunos casos imposible de realizar.
EXPERIAN EQUIFAX y ASNEF	-Habilitación expresa o Interés legítimo tanto para ficheros de solvencia positivos como negativos.Determinar requisitos de inclusión de datos negativos. -Mantenimiento de la obligación de enviar requerimiento previo de pago (con mejoras técnicas) -Mantenimiento de la ausencia de disputa sobre la deuda (con mejoras técnicas) -Mantenimiento del deber de notificar la inclusión de datos negativos y de los criterios del actual 40 RGPD (con mejoras técnicas) Deberes de información del acreedor/entidad informante. - Mantenimiento del deber de informar sobre la consulta del actual art. 39 RLOPD (con mejoras técnicas) - Mantenimiento del deber de informar sobre la aportación del actual art. 42.2 RLPD (con mejoras técnicas) -Excepción al deber de informar respecto de los ficheros de solvencia regulados en el art. 29.1 LOPD.

	-Mantenimiento de los requisitos previstos en el actual art. 42, 1. b). Ampliación a los supuestos de localización de un deudor. -Decisiones automáticas / elaboración de perfiles Nueva regulación que establezca derechos y garantías para los afectados, sobre la base del art. 22,2,a) RGPD -Mantenimiento del régimen de responsabilidades del art. 43 RLOPD, sobre la base de la "corresponsabilidad" del art. 26 RGPD. -Plazo de permanencia de los datos en los ficheros.Ampliación del plazo de permanencia de 6 años del art. 29.4 LOPD a 10 años como la Central de Información de Riesgos. - Supresión de la prohibición del Saldo "0". - Regulación de la posibilidad de cobrar los derechos de acceso bajo ciertas circunstancias. - Regulación del plazo y procedimiento en el derecho de supresión y rectificación. - Modulación del derecho de oposición y limitación del tratamiento en los ficheros de solvencia. -Fuentes accesibles al público y registros públicos.Reconocimiento expreso de que los datos procedentes de boletines oficiales y similares, y ciertos registros públicos con información relevante pueden ser incluidos en los ficheros de solvencia,
ADIGITAL	-necesario **establecer una clara diferenciación entre las dos modalidades de consentimiento.** -En lugar de crear una lista de casos en que estaría justificado el interés legítimo para tratar datos, sería necesario garantizar una **legislación basada en principios**, sin que ello signifique conceder a los responsables del tratamiento la capacidad de determinar de manera unilateral cuándo son legítimos los intereses.

	-estimamos conveniente que la nueva norma española adopte la edad de **13 años** como límite para el consentimiento de los menores. -**el consentimiento necesario para el tratamiento de los dispositivos de almacenamiento y recuperación de datos (cookies)** está regulado en la Directiva 2002/58, desarrollada en la Ley de Servicios de la Sociedad de la Información. Sería conveniente que la norma de adaptación española incluyese expresamente esta interpretación a fin de garantizar la seguridad jurídica y evitar conflictos de interpretación. -el derecho de información regulado en el Reglamento debe interpretarse de forma que sea compatible con los secretos comerciales, industriales y la propiedad intelectual. -El tipo de datos sobre los que se aplicaría el derecho de portabilidad es excesivamente amplio. - necesario que la nueva **norma aclare el ámbito territorial del derecho de supresión** y cómo debería ser implementado en el marco europeo. -conveniente que la nueva norma recoja un criterio para determinar **qué son fuentes de acceso público y no una lista cerrada que quedaría obsoleta en poco tiempo.** -especifique que **la manifestación de oposición del usuario sea un criterio válido para el cese de la conservación de datos**. **Debe permitirse a los responsables conservar la lista de los usuarios que se han opuesto** a los tratamientos con la finalidad de prevenir posibles tratamientos posteriores. -sería necesario permitir que el contrato entre el responsable y el encargado del tratamiento pudiese contener **una cláusula que habilite al encargado a recurrir a subencargados sin necesidad de informar al responsable**, siempre y cuando, en la elección de éstos, adopte las garantías necesarias para mantener el nivel adecuado de protección de los datos. Así mismo, **el contrato debería permitir a las partes regular el grado de implicación del responsable en la realización de auditorías e inspecciones**. La responsabilidad conjunta debe quedar limitada a aquellos supuestos en los que el encargado del tratamiento esté gestionando datos del responsable y le esté dando asistencia. -toda ampliación de los casos en los que se obliga al responsable a disponer un de delegado de protección de datos, debe ser ejercida en consenso y de forma coordinada con el resto de los Estados Miembros y únicamente en supuestos

	excepcionales. -Lo mismo respecto de las evaluaciones de impacto. Necesidad de modelos y guías. Precisar **"alto riesgo".** Las evaluaciones de impacto también deben considerar los **beneficios** para los interesados y no únicamente los riesgos. Es esencial que **la eventual obligación de consultar a los interesados o sus representantes no perjudique a los intereses comerciales de los representantes, en especial los relativos a la seguridad y a los derechos de propiedad intelectual** -la nueva norma **debe recoger criterios para la graduación de las sanciones** como, por ejemplo, considerar los perjuicios causados. En base a esos criterios y a la proactividad y cautela del responsable **consideramos adecuado mantener en la normativa española la figura del apercibimiento,** siempre que se aporten las adecuadas garantías, como la adhesión a códigos de conducta o la implementación de sistemas de gestión. -fijar criterios sobre la anonimización -establecer el mecanismo de ventanilla única
CAIXABANK	- Tipificación: es excesiva amplia (genérica) lo que entraría en contradicción con sistema jurídico penal y administrativo sancionador español. Por tanto, la normativa nacional debe desagregar los tipos infractores. Lo mismo ocurre en relación a la graduación de las penas y la prescripción de infracciones y sanciones. La extensión de los tipos que contempla el RGPD resulta incompatible con la exigencia de proporcionalidad en el ámbito administrativo sancionador -Los tratamientos de datos estrictamente necesarios en la actividad de las entidades financieras han de quedar exentos. Se incluye un listado no limitativo de las normas que deben cumplirse que deberían quedar exoneradas. -consentimiento en menores de edad: debe fijarse la edad en los **14 años.**
APEP	Dado que se ha aprobado un Reglamento y no una Directiva, es evidente que la intención no es fomentar iniciativas nacionales que fragmenten el mercado interior en la UE. La iniciativa no debe tampoco perder de vista la dependencia que el mercado interior tiene respecto de la innovación.
UNIVERSITAT DE BARCELONA	-artículo 10 de la LOPD: sólo un conjunto de profesionales están sujetos a secreto profesional, por ejemplo, médicos o abogados. Para evitar que se pueda interpretar como que aquellas profesiones que no tengan secreto profesional no

	deben mantener el deber de secreto, quizás sería interesante eliminar “profesional” del artículo 10. Por ejemplo, en el artículo 90.1 del RGPD se hace distinción entre “obligación de secreto profesional” y “otras obligaciones de secreto equivalentes”.
AEB ASOCIACIÓN ESPAÑOLA DE BANCA	**Consideraciones generales** -aclarar aquellos conceptos cuya aplicación práctica plantea dudas: las obligaciones relacionadas con el consentimiento y la portabilidad. - **El cumplimiento de la labor de colaboración de las entidades en la prevención del delito de blanqueo de capitales y financiación del terrorismo hace necesario eximir de la exigencia de consentimiento expreso e inequívoco de los clientes para la cesión de datos en determinados supuestos**. - Por lo que se refiere a los proveedores de servicios de pago, las nuevas disposiciones legales deben aclarar qué régimen jurídico es aplicable a aspectos como la portabilidad de los datos. - Sin perjuicio de todo lo anterior, la nueva legislación debería guiarse por el principio de intervención mínima. - plena coherencia entre la legislación específica de protección de datos y las disposiciones sobre esta misma materia recogidas en la normativa sectorial sobre prevención del blanqueo de capitales, vídeo vigilancia, servicios de pago, seguros, etc. **- Consentimiento:** necesario aclarar los términos en los que se entenderá otorgado el consentimiento de forma implícita y, por tanto, se permite, dado que pueden surgir dudas para calificar un consentimiento de tácito, prohibido, o implícito, permitido. Se proponr que se incluya en la ley española una disposición que establezca que el tratamiento de datos personales para fines de mercadotecnia directa, o comerciales, se pueda continuar realizando sin tener que recabar de nuevo el consentimiento de los interesados, cuando éstos sean ya clientes de la entidad responsable del tratamiento en la fecha de entrada en vigor del Reglamento. **- Decisiones individuales automatizadas** -qué **requisitos debe cumplir la decisión** para que se considere basada únicamente en el tratamiento automatizado puesto que la mayoría de decisiones automatizadas contemplan en alguna parte del proceso -bien en la configuración de los parámetros, bien al final- una intervención humana.

	La segunda duda es **qué debe entenderse por qué produzca efectos jurídicos al interesado o le *afecte significativamente***. En estos casos, además de que la nueva norma deberá detallar el alcance de la explicación a facilitar al titular de los datos sobre la lógica aplicada, debe plantearse que en ella se recoja también la salvedad lógica de excluir del conocimiento del interesado toda la información generada por la propia entidad a partir del tratamiento de datos y aquélla que el responsable no deba revelar por razones de seguridad. En todo caso deberá excluirse aquella información sobre la que el responsable ostente derecho de propiedad intelectual o constituya un secreto comercial de la compañía. **- Portabilidad** -resulta necesario prever expresamente los términos de aplicación de las disposiciones específicas sobre el derecho de **portabilidad para el sector financiero** ya que, en el ámbito de los servicios de pago, existe normativa que ya regula el acceso a datos. - **los nuevos conceptos que introduce el derecho de portabilidad regulado en el RGPD son tan genéricos** que dan lugar a multitud de interpretaciones y, en consecuencia, trasladan una inseguridad jurídica a la hora de su aplicación. -debería hacerse una aclaración sobre qué incluyen los **datos observados** y limitar su alcance incluyendo una definición de ese término teniendo en cuenta las obligaciones por normativa específica nacional. -Es importante definir qué se entiende por "técnicamente posible". -conveniente prever la definición de unos estándares técnicos que permitan a los responsables del tratamiento la elaboración de un formato estructurado, de uso común y lectura mecánica que sea "interoperable" y reconocible por todos ellos. - establecer normas específicas de portabilidad que permitan a determinados sectores que tratan datos sensibles, como el sector financiero o el de sanidad. -excluir del derecho de portabilidad del interesado determinados datos, ya sea por razones de seguridad u otras que hagan conveniente su no revelación y entrega al interesado. **- Prevención del blanqueo de capitales** -además de mantenerse las normas vigentes, se adopten las siguientes disposiciones:- no será preciso el consentimiento del afectado cuando el tratamiento tenga por finalidad la aplicación por parte de los sujetos obligados de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, de las

	medidas de diligencia debida sobre las personas físicas y jurídicas con las que pretendan establecer relaciones de negocio o intervenir en cualesquiera operaciones; no será necesario el consentimiento del afectado para la comunicación de datos a terceros; cuando la cesión de datos se produzca para la aplicación de las medidas de diligencia debida previstas en el Capítulo II de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, siempre que la cesión se produzca entre sujetos obligados de la citada Ley; cuando la cesión de datos se produzca, en los términos que se determinen reglamentariamente, entre administraciones públicas y sujetos obligados de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, para la aplicación de las medidas de diligencia debida previstas en dicha ley. En todo caso resulta imprescindible autorizar expresamente la transferencia o cesión, entre empresas de un mismo grupo, de cualquier información relacionada con la prevención del blanqueo de capitales y la financiación del terrorismo, incluida la resultante de la aplicación de las medidas de diligencia debida. Se sugiere considerar la posibilidad de: - Incluir expresamente una excepción a la obligación de informar cuando los datos no hayan sido facilitados por el interesado, garantizando sus derechos y libertades (art. 14 RGPD). - Concretar los casos en los que por mandato legal se han de suprimir los datos confidenciales (art. 17 RGPD). - Limitar específicamente los casos en los que se ha de informar de la violación de seguridad de los datos al interesado (art. 23 RGPD).En relación con esta materia podría ser conveniente establecer un procedimiento/ listado de acciones a llevar a cabo dentro del plan de alerta temprana (72 horas) si una empresa es ciberatacada; y precisar los documentos que la empresa deberá aportar a la Autoridad de Control (en España la Agencia Española de Protección de Datos) para acreditar su diligencia.En el caso de que durante esas 72 horas no se haya podido determinar la causa objeto del ciberataque, porque se necesite más tiempo para documentarla, debería recogerse que si la investigación está en curso y no se puede aportar el informe de la investigación en ese plazo de tiempo, la empresa no será sancionada hasta que no se llegue a un resultado concluyente. - Recoger especialidades en el tratamiento de datos en el ámbito laboral teniendo en cuenta la doctrina y jurisprudencia existente que no contradiga la nueva regulación. (art. 88 RGPD). - Incluir regulación específica, adaptada al nuevo ordenamiento, respecto de los ficheros de cumplimiento e incumplimiento de obligaciones dinerarias.
AMETIC Asociación de Empresas de Electrónica, Tecnologías de la Información, Telecomunicaciones	**-Determinar con claridad tanto el procedimiento sancionador local como los importes o escala de importes de las multas**, ya que el Reglamento contiene un arco muy amplio de multas. -Aclarar en qué forma y cómo va a funcionar el procedimiento de **resolución extrajudicial de conflictos en los códigos**

y Contenidos Digitales,	**tipo**, ya sean de empresas o sectoriales.
MICROSOFT	-La LOPD y el RLOPD han sido un referente a nivel europeo por su grado de desarrollo y aplicación, por lo que es conveniente que la futura legislación mantenga el principio de horizontalidad sobre los distintos ámbitos de aplicación manteniendo una estrecha coordinación y coherencia con la legislación relacionada en la materia, evitando así una fragmentación normativa innecesaria para el ordenamiento español. -Armonización: Consentimiento en el tratamiento de datos de menores.Para evitar una fragmentación que pueda desproteger a los niños consideramos que las autoridades españolas deben trabajar de manera coordinada con los Estados miembros y la industria para definir de manera uniforme dicha edad correspondiente en España. Una vez definida, es importante que las autoridades españolas establezcan las pautas para verificar el consentimiento otorgado por los padres o tutores legales de los menores. Dichas pautas deben ser confiables, predecibles y seguras y deben evitar ser onerosas o complejas tanto para los representantes legales de los menores como para las empresas . -delimitar el alcance de tratamientos de alto riesgo señalados en el artículo 35.1 del Reglamento. -La legislación de implementación deberá ser **flexible** respetando los principios del Reglamento y permitir mecanismos sencillos para demostrar la existencia de interés legítimo basado en las expectativas razonables de la prestación de servicios de que se trate. -establecer las pautas para la Pseudonimización. -en materia de **seguridad** el Esquema Nacional de Seguridad (Real Decreto 951/2015 del 23 de octubre) que establece los requisitos para la seguridad y protección de la información, contiene de manera objetiva los elementos necesarios para dar cumplimiento a las obligaciones que sobre seguridad impone el Reglamento y por ello puede ser claramente un referente a nivel europeo que garantice una armonización sobre la materia.
DERECHOS ARCO (asesoría jurídica)	- **Transferencias internacionales de datos de carácter personal**: concretar si la autorización se llevará a cabo en relación al contrato, pudiéndose emplear en varias transferencias internacionales con base en el mismo contrato autorizado, o por el contrario requerirá autorización para cada una de las transferencias. -Exclusiones a la aplicación: datos profesionales referidos a personas jurídicas, o a los ficheros que se limiten a incorporar los datos de las personas físicas que presten

	sus servicios en aquellas. Especialmente relevante para la operativa de las entidades, será la especificación de excepciones en este sentido. -Procedimiento sobre la **evaluación de impacto**, programa de cumplimiento normativo, y auditorias técnicas. Es necesaria la identificación tanto de tipos de operaciones de tratamiento que requieran una evaluación de impacto, como de los criterios de identificación de las mismas cuando no se encuentren tasadas. **No existe mención en el RGPD a las auditorias de cumplimiento, por lo que se agradecería una especificación local en este sen**tido, siendo necesario definir cuáles van a ser los plazos dirigidos a efectuar tales auditorías (internas o externas) y en su caso eventuales medidas de seguridad adicionales. -**Tratamiento de datos en el ámbito laboral** :definir aquellos tratamientos cuya finalidad se entiende inherente a la relación laboral, no requiriendo el consentimiento, así como aquellas finalidades que así lo requieren y de qué forma (expresa o tácita) y el establecimiento de excepciones a la aplicación de determinadas medidas de seguridad, como concurre actualmente respecto de los datos de afiliación sindical o discapacidad, por ejemplo. -**Procedimiento para los organismos certificadores y la obtención de certificados** cabe plantearse la posibilidad de extender el sistema nacional de seguridad y adecuarlo a la nueva normativa salvo que resulte realmente necesario fijar otro sistema de certificación. -**Obtención del consentimiento cuando concurren varias finalidades. Su regulación** aportaría seguridad jurídica a las empresas
FUNDACIÓN FIDE	-Coordinación y armonización con la legislación sectorial y autonómica. -criterio de “mínima intervención” -regulación de algunas cuestiones en Códigos de conducta en vez de en ley.
SIGACUS GESTIÓN, S.L.	**-no se suprima la obligatoriedad** de **inscripción de ficheros** de datos personales por parte de los Responsables de Tratamientos en el **Registro General de Protección de Datos** de la Agencia Española de Protección de Datos.

IAB SPAIN	-**el interés legítimo debería configurarse como la base jurídica fundamental para el tratamiento de datos** en la futura ley de protección de datos en España, **ya que es la única forma de legitimar el tratamiento cuando no es posible obtener el consentimiento del usuario**. Ha de regularse de forma flexible y no mediante lista cerrada. -**el consentimiento** necesitará ciertas aclaraciones sobre su aplicación, dado que el texto se refiere a un consentimiento expreso y uno implícito sin determinar los límites de ambos. La futura ley debería contener mecanismos operativos por los que, con las garantías adecuadas, autorice a los responsables a seguir usando esos datos que se recogieron con el consentimiento, y sobre todo aquellos que se recabaron con el consentimiento tácito -la edad de consentimiento d elos menores será de **13 años**. - aclarar la portabilidad de datos -derecho de supresión: es necesario que la ley aclare algunos aspectos, como el ámbito territorial cómo debe implementarse en la Unión Europea, y su interrelación con jurisdicciones de países extracomunitarios que no reconocen, no regulan, o lo hacen de manera diferente, este derecho. Una solución a tener en cuenta puede ser el uso de la geolocalización para restringir el acceso a las URLs bloqueadas en todos sus dominios, que cumple con los criterios del TJUE. - Ventanilla única y mecanismos de colaboración funcionamiento de este mecanismo sea en coordinación de todas las autoridades de protección de datos europeas.
ASOCIACIÓN ESPAÑOLA DE STARTUPS	-el objetivo debe ser no complicar y recargar la regulación para reducir la incertidumbre de las empresas, que es lo peor para el desarrollo empresarial y proteger los derechos de los ciudadanos. -También es preciso estudiar las excepciones sectoriales, ya que muchas de las nuevas empresas innovadoras no encajan en ningún sector, son híbridos transversales y no podrán innovar si tienen que cumplir distintas regulaciones para cada uno de los sectores que tocan.

	- las multas previstas (20 millones de euros o un % de la facturación total, lo que sea mayor) serían inasumibles para la gran mayoría de las empresas..
ISMS FORUM SPAIN-DATA PRIVACY INSTITUTE	--conviene aclarar si los datos de los profesionales autónomos y empresarios individuales en el ejercicio de su actividad y los datos de contacto de personas físicas que desempeñen su trabajo en personas jurídicas (referidos a su nombre y apellidos, puesto de trabajo/cargo, teléfono y email corporativos) continuarán exentos. -debe contemplar, como lo hace actualmente, el tratamiento de datos de solvencia patrimonial y de crédito o de los ficheros comunes de exclusión del envío de comunicaciones comerciales (ficheros Robinson). -la renovación del consentimiento ya otorgado de forma previa a la entrada en vigor del Reglamento, no debería imponerse de forma obligatoria, pudiendo plantearse su validez y, en su caso, posible convalidación en base a los mecanismos y cauces que permite el propio RGPD. -se debe atender al principio de la irretroactividad de las normas restrictivas o sancionadoras, -en principio la norma no debería aplicarse a situaciones pasadas, pudiendo ser válidos los consentimientos obtenidos al amparo de la anterior legislación aplicable. -El Reglamento no admite el consentimiento tácito ni las casillas marcadas (considerandos 32 y 43 y artículos 4 y 7). Para materializar el consentimiento expreso o explícito que parece exigirse resulta necesario aclarar los siguientes aspectos: - Alcance de las expresiones “cuando el tratamiento tenga varios fines, debe darse el consentimiento para todas ellas” y “autorizar por separado las distintas operaciones de tratamiento de datos personales” (considerandos 32 y 43). Parece dar a entender que deben recabarse varios consentimientos, uno por finalidad. - El artículo 4 indica que la solicitud de consentimiento debe presentarse “de forma que se distinga claramente de los demás asuntos”: ¿a qué distinción se refiere?, ¿sería válida una cláusula específica al respecto ya sea dentro del contrato o como anexo? La nueva regulación debe contemplar, como lo hace actualmente, el tratamiento de datos de solvencia patrimonial y de crédito o de los ficheros comunes de exclusión del envío de comunicaciones comerciales tal como la lista Robinson. Debido a que **el nuevo reglamento incorpora derechos que no existen a día de hoy en la ley española (como el derecho al olvido o a la portabilidad)** desde la totalidad de las empresas **se considera inviable iniciar la recogida de**

	dichas actualizaciones antes de que entre en vigor la norma. Sin embargo, si se espera a dicha fecha se estaría incurriendo en una falta grave. Por ello, se considera que es necesario un **periodo de adaptación** consecuente con las obligaciones introducidas, no inferior a tres meses -Sería conveniente **modular o adaptar la definición de las categorías especiales de datos recogida en el artículo 9 y, por lo tanto, la protección de los mismos de acuerdo a la finalidad de su tratamiento.** Por ejemplo, los datos biométricos, fotografías, etc., recabados con la finalidad exclusiva de identificación de los individuos, o los datos de afiliación sindical con la finalidad exclusiva de pago de nóminas. ¿Realmente deben considerarse datos de categoría especial con todas las obligaciones correspondientes? -Tratamiento que no requiere identificación. Es un nuevo supuesto de tratamiento (artículo 11) cuyo alcance no se entiende. Respecto al deber de transparencia recogido en el artículo 12.2 para este supuesto de tratamiento, ¿a quién se va a informar y a qué interesado se refiere si como RF no podemos identificar? En algunos casos, nos encontramos con que los datos sensibles no pueden tratarse al amparo del interés legítimo, sin embargo, puede darse la circunstancia de que no sea posible recabar el consentimiento con carácter previo al tratamiento de los datos personales. En este caso, ¿Cómo se articula? -Deber de Información -¿cómo acreditarlo en el caso de información verbal? - Se posibilita que la información se entregue en combinación con iconos normalizados ¿A qué se refiere exactamente y cómo operan dichos iconos? -Por lo que se refiere a los nuevos aspectos sobre los que necesariamente debe ser informado el interesado, destacamos los siguientes puntos: - Base jurídica del tratamiento (considerandos 41, 47 y 48): se indica que no tiene que ser un “acto legislativo adoptado por un parlamento” pero no se define con claridad el concepto. Es necesariauna definición concreta y clara del mismo y una determinación de los supuestos en los que se considera que concurre el interés . - Plazo de conservación de los datos o criterios utilizados para determinar este plazo: ¿Cabe una remisión genérica al plazo de prescripción de las acciones legales establecido en la normativa vigente o debe determinarse el plazo de

	conservación en función de los colectivos afectados (clientes, empleados, proveedores, etc.) y/o de las finalidades del tratamiento (desarrollo de un contrato, videovigilancia, control de accesos, etc.)? Sería conveniente una mayor concreción de los criterios a utilizar para determinar dichos plazos, especialmente para los tratamientos que entrañen mayor riesgo. -Lógica utilizada y consecuencias en la elaboración de perfiles de clientes: entendemos que son conceptos que deben concretarse para determinar el alcance de la información a facilitar. -Transferencias internacionales: conviene concretar la obligación de informar a los interesados sobre cómo localizar o dónde consultar las garantías en las que se basa el RF o el ET para amparar las transferencias internacionales de sus datos personales. -En relación a los nuevos derechos que el Reglamento reconoce a favor de los interesados deben desarrollarse los siguientes aspectos: - ¿Todo derecho de supresión (artículo 17) se entiende que conlleva el derecho al olvido o debe ser solicitado este último también por el interesado de forma expresa?. ¿Cuál es el alcance de las "medidas razonables" a adoptar para informar a los responsables de la solicitud del interesado de cancelación de cualquier enlace a los datos o de copia/réplica de los mismos?. ¿No se prevé el bloqueo previo de los datos previsto en el RLOPD?. - ¿Cuál es el alcance del derecho de limitación (artículo 18)?. ¿Cuáles son los supuestos en los que el responsable ya no necesita los datos, pero sí el interesado que obliguen al RF a mantener la información? - ¿Qué datos concretos se entienden afectados por el ejercicio de un derecho de portabilidad (artículo 20), con qué alcance, cómo debe materializarse, qué medidas de seguridad deben adoptarse en la transmisión de los datos? Nos remitimos en este sentido a las observaciones enviadas a UNESPA sobre el documento específico de Insurance Europe relativo a este derecho. - Cuando se indica que el derecho de oposición debe "ser mencionado explícitamente al interesado y al margen de cualquier otra información", ¿a qué se refiere?, ¿no cabe la información sobre este derecho junto al resto de los derechos? Por otro lado, parece obligarse al RF a admitirlo en todo caso en los supuestos de oposición para fines de mercadotecnia (artículo 21.3), ¿esto no es contradictorio con la consideración de la mercadotecnia directa como interés legítimo que se recoge en el considerando 47?. Interés legítimo Principio de Responsabilidad Proactiva: deben especificarse las "medidas apropiadas" para garantizar que el tratamiento se realiza conforme a lo dispuesto en el Reglamento, más allá de la mención que se hace a códigos de

	conducta o certificaciones que aún no están desarrolladas. De igual modo, no se especifica el nivel de documentación que deberán tener disponible las entidades en relación al tratamiento de la información y las medidas de seguridad asociadas, lo que podría denominarse un "documento de seguridad ampliado" que permita acreditar este concepto de diligencia debida. Sería conveniente, en aras de la seguridad jurídica, especificar al menos medidas técnicas y organizativas concretas que hagan viable acreditar que el tratamiento es conforme con el Reglamento, y que faciliten la prueba de ese cumplimiento ante requerimientos de la APD, con independencia de desarrollo de certificaciones y de códigos de conducta. -Se requiere una **aclaración de los conceptos de seudonimización y cifrado de datos** para un mejor entendimiento de la diferencia entre ambos (artículo 32), de su alcance y de las ventajas de su aplicación por el RF. -conveniente que otras medidas como la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento o de restaurar la disponibilidad y el acceso de forma rápida, fueran concretadas en la nueva normativa, así como determinar qué medidas de seguridad de las que actualmente se recogen en la LOPD y RLOPD deberán mantenerse. -Evaluación del impacto en caso de alto riesgo: sería conveniente detallar el alcance y metodología a emplear en cada caso, así como concretar los supuestos en los que se considerará que concurren los diferentes niveles de riesgo -Comunicación de violaciones de seguridad ¿Qué se considera una violación de seguridad? Creemos importante su definición para confirmar que no todo incidente será considerado como tal y quede sujeto a las obligaciones de comunicación establecidas en los artículos 33 y 34 del Reglamento. De igual modo, la nueva normativa debería determinar con exactitud los supuestos en los que se considera que existe riesgo (artículo 33) y riesgo alto (artículo 34) para los derechos y libertades de los interesados que obliguen al RF a realizar la notificación de la violación de seguridad a la autoridad de control y/o al interesado. -Habría que determinar cuánto margen de negoción existe para el Encargado del Tratamiento y, en caso de implementar medidas que no sean suficientes, quién responde y si el Responsable del Fichero va a tener alguna responsabilidad por deber de diligencia.

	-Se deberían concretar los aspectos que deberán ser tenidos en consideración para la elaboración de un código de conducta asociado a un sector determinado. De igual modo, se deberá establecer el periodo de adaptación y las acciones que habrá que realizar de cara a la regularización de los códigos tipos actualmente en funcionamiento. -¿Cabe la acción judicial directa de los interesados sin previa denuncia ante la APD? (artículo 79 y considerando 145). ¿Cómo evitar la doble sanción por los mismos hechos bajo el principio de "non bis in ídem"? ¿Cómo se va a articular la nueva reclamación de indemnización por daños yperjuicios que contempla el Reglamento y cuya responsabilidad establece de forma solidaria para todos los RF/ET que hayan participado en la operación de tratamiento? (artículo 82 y considerando 146). -La nueva normativa deberá concretar las normas en materia de "otras sanciones" (artículo 84) aplicables a las infracciones del Reglamento, en particular las infracciones que no se sancionen con multas administrativas. -concretar que hechos tendrán la consideración de infracción y la calificación de las mismas según su gravedad al objeto de determinarse la sanción aplicable (sea multa administrativa o cualquier otra). -En cuanto al calado o nivel de las sanciones, el artículo 83 hace referencia a sanciones bajo el término "Global", por lo que cabe aclaración sobre si se trata de la facturación global de la empresa o de la facturación global a nivel de grupo empresarial. -Asimismo, los plazos de prescripción de las infracciones y sanciones. - necesidad de determinar el las certificaciones de profesionales de la protección de datos ya existentes en el sector. -Edad en que los menores podrán disponer de su información personal -podría resultar realista bajar la edad de 14 a 13 años
AMERICAN CHAMBER OF COMMERCE IN SPAIN	**Ventanilla única**: Para mayor claridad, cuando una organización designe una ubicación como su sede principal, presumiblemente, debería considerarse la "sede principal".

	Tratamiento de alto riesgo y Evaluaciones de impacto relativas a la protección de datos (DPIA): Es necesario proporcionar información adicional en cuanto a lo que constituye un "tratamiento de alto riesgo". **Violaciones de seguridad de datos personales y notificaciones**: Se necesitan directrices en cuanto a los tipos de violaciones de seguridad que entrañan un "riesgo" que requiera una notificación a las Autoridades encargadas de la Protección de Datos (DPA), y qué factores adicionales entrañan un "alto riesgo" que requiera una notificación a los interesados. **Códigos de conducta aprobados y certificación**: Deben ser pragmáticos y nunca deberían ser menos flexibles que las normas básicas del GDPR. **Portabilidad de datos**: Las directrices deberían aclarar que el derecho ampara únicamente a aquellos datos proporcionados por los interesados pero no a los datos generados por el servicio. **Sanciones**: El Comité Europeo de Protección de datos (EDPB) debería respaldar un uso equilibrado de todo el espectro de poderes y un diálogo con los distintos sectores empresariales. **Delegados de protección de datos (DPO)**: Las directrices deberían aclarar, en particular, el significado de los términos "actividades principales" y "tratamiento a gran escala".
DESPACHO NAVARRO	-Disminuir los deberes de información y consentimiento expreso de personas de contacto de empresas, profesionales, empresarios, comerciantes y en general todos los cargos públicos cuyos datos están en webs o registros oficiales. La vida comercial se complica excesivamente puesto que el envío de información, invitaciones etc. es el día a día de la mayoría de empresas.
ÁUDEA SEGURIDAD DE LA	**"Datos biométricos**" (art. 4.14 del RGPD) debe especificarse claramente que dichos datos serán considerados como categorías especiales de datos cuando pretendan la identificación unívoca de un interesado (conforme al Considerando

INFORMACIÓN, S.L.	51 del RGPD). De lo contrario, cualquier foto de una cara de una persona podría considerarse como una categoría especial de datos. **"Interés legítimo":** los supuestos o ejemplos sean concretos o que se den pautas para identificar correctamente aquellos supuestos en los que hay un "interés legítimo", en lugar de dejar la interpretación de este concepto a la discrecionalidad de las autoridades de protección de datos. **Acreditación de la obtención del consentimiento (art. 7.1 del RGPD)** : deberían regularse las formas de acreditar el consentimiento. **Consentimiento del niño** (art. 8 del RGPD): proponemos los 13 años. **"Manifiestamente públicos**" (art. 9.2.e) del RGPD) concretar qué debe considerarse por "manifiestamente públicos y qué consecuencias tiene. ¿Habría que obtener un consentimiento inequívoco? ¿Bastaría con informar? ¿Constituirían Fuentes Accesibles al Público? **Regulación del "canon razonable**" previsto para ejercicio de derechos infundados o excesivos (arts. 12.5 a) y 15.3 del RGPD) Sería necesario que la nueva normativa estableciera cómo determinar este canon y en qué casos podrá aplicarse. **Contenido y alcance del derecho de Acceso** (art. 15 del RGPD) conveniente que la nueva norma se pronuncie sobre el contenido y alcance de este derecho, con expresa mención a si dicho alcance incluye o no los datos elaborados por las empresas, como por ejemplo, perfilados, combinaciones, inferencias, valoraciones, transformaciones de los datos facilitados por el afectado, y datos generados automáticamente (logs, líneas de comando, etc.) **Derecho de Supresión vs. Derecho de Cancelación** (art. 17 del RGPD) la nueva norma ha de regular la fase del bloqueo de los datos para garantizar una adecuada seguridad jurídica. **"Efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar"** (arts. 22 y 66 del RGPD) El alcance de esta condición debe quedar claramente delimitado en la norma española. **"Privacidad por defecto y desde el diseño" (art. 25 del RGPD)** surgen dudas con respecto a la prohibición de que los datos sean accesibles para un número indeterminado de personas sin intervención del afectado.Existen determinados servicios que, por su naturaleza, implican necesariamente la publicación de datos personales de forma que sean accesibles para un número indeterminado de personas, como por ejemplo: foros, noticias, comentarios en noticias, redes sociales, etc. Se sugiere una regulación menos agresiva, al menos para aquellos servicios cuya propia finalidad implique la difusión consciente de la información publicada por un usuario. "**Registro de Actividades de Tratamiento" (art. 30** del RGPD)¿Deben considerarse "trabajadores" los estudiantes que realizan prácticas formativas (becarios)? ¿y los trabajadores externos cuya nómina depende de una tercera empresa? **"Nivel de seguridad adecuado al riesgo"** (art. 32 del RGPD) se regule claramente los niveles y medidas de seguridad, tal y como se hace en el Título VIII del RLOPD actualmente.Lo contrario podría implicar una gran inseguridad jurídica

	para las empresas cuyo criterio de "nivel de seguridad adecuado" no concuerde con el de la autoridad de protección de datos. **"Consulta Previa"** (art. 36 del RGPD) que la nueva norma regule claramente en qué casos será necesaria esta consulta previa **"Gran escala"** (arts. 27, 35 y 37 del RGPD)Es necesaria una aclaración más orientativa sobre este asunto. **"Actividades Principales**" (art. 37 del RGPD) La diferencia entre actividades principales y auxiliares debería quedar aclarada de forma que no quede tan expuesta a interpretaciones más o menos arbitrarias. **"Observación Sistemática"** (arts. 35 y 37 del RGPD) la Guía del GT29 ofrece una interpretación cerrada y prolija que debería ser incorporada a la legislación española **"Dilación indebida**" (art. 34 del RGPD) el artículo 34 se limita a exigir que se informe a los interesados "sin dilación indebida". Consideramos necesario aclarar este plazo para comunicar las brechas de seguridad a los afectados. **Representación de los Interesados (art. 80 del RGPD)** la nueva norma debería especificar claramente para evitar confusiones que no se excluye la representación voluntaria o legal por medio de asesores, abogados y/o despachos profesionales. **Régimen sancionador** (art. 83 del RGPD) se establezca un régimen sancionador similar o equivalente al recogido actualmente en Título VII de la LOPD y que los límites máximos del régimen sancionador del RGPD se restrinjan únicamente a grandes compañías y grupos multinacionales. Asimismo, debería regularse si las Administraciones Públicas podrán ser objeto de sanción económica y bajo qué condiciones. **"Volumen de negocio total anual global**" (arts. 83.4 y 83.5 del RGPD) Consideramos conveniente que la norma española determine si estos porcentajes se refieren al resultado individual o al consolidado en el caso de grupos de empresas (conforme al artículo 42 del Código de Comercio). **Regulación específica de la libertad de expresión y de información** (art. 85 del RGPD) consideramos conveniente que en España se regule adecuadamente a los tiempos actuales el conflicto existente entre la libertad de expresión y de información y el derecho a la protección de datos, teniendo especialmente en cuenta el tratamiento necesario en los medios de comunicación social. **Regulación específica del tratamiento del DNI** (art. 87 del RGPD) **Regulación específica del tratamiento de datos personales de los trabajadores en el ámbito laboral** (art. 88 del RGPD) teniendo especialmente en cuenta los flujos (incluso internacionales) entre empresas de un mismo grupo empresarial. **Regulación de los ficheros estadísticos, históricos o científicos** (art. 89 del RGPD) sería conveniente dilucidar si se incluirán dentro de esta categoría aquellos ficheros relacionados con los estudios de mercado realizados por entidades privadas, ya sea por su propia iniciativa o a instancia de terceros. Debería tenerse en cuenta que el cumplimiento del deber de información tal y como lo exige la normativa actual y también el RGPD, podría suponer un sesgo en el estudio

	de mercado invalidando los resultados del mismo. **CUESTIONES NO PREVISTAS EN EL RGPD** -el RGPD supone un paso atrás en muchas cuestiones que han de mantenerse en la legislación española: **Excepciones del 2.3 y 2.3 del RLOPD** Es necesario que la nueva norma resuelva la cuestión referida a este tipo de tratamientos. En nuestra opinión, resulta razonable y pertinente el mantenimiento de dichas excepciones siempre y cuando la finalidad sea el contacto y las relaciones entre empresas que utilizan mecanismos de contacto asignados circunstancialmente a personas físicas. -**Consentimiento de los padres, madres o tutores legales de los menores** (art. 13 RLOPD) (…)4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales." Esta carga ha sido uno de los aspectos más criticados del actual RLOPD, pues no existe ninguna forma factible de cumplir en el entorno online con registros automatizados y masivos. Cualquier formulario online es susceptible de captar datos de menores de 14 años (incluyendo los formularios de las propias autoridades de protección de datos).Consideramos necesario regular de forma específica cómo solucionar este problema en el entorno online. **Solicitud del consentimiento en el marco de una relación contractual** para fines no relacionados directamente con la misma (art. 15 del RLOPD) es conveniente que la nueva norma mantenga la regulación vigente o que, en su defecto, defina claramente cómo deben obtenerse estos consentimientos. **Regulación específica de los "Ficheros de solvencia patrimonial y crédito"** es necesario que sean claramente regulados, ya que en la actualidad son la principal fuente de infracciones y sanciones por parte de la AEPD. **Regulación específica de los "Ficheros con fines comerciales**" En el RGPD no existe mención alguna (a excepción del encuadre del marketing directo dentro de la base legal del interés legítimo, conforme al Considerando 47 del RGPD) y es necesario que estos tratamientos sean claramente regulados. **Regulación de los "Prestadores de servicios sin acceso a datos"** Sería conveniente su regulación en una línea similar a la actual. **Regulación específica de la Videovigilancia** (Instrucción 1/2006 de la AEPD) es conveniente que la nueva norma regule claramente estos tratamientos, con pronunciamiento expreso sobre la base legal en la que se amparan (por ejemplo, el interés legítimo), ya que no será posible amparar los sistemas de videovigilancia en el consentimiento tal y como se regula en el RGPD. **Regulación específica de los derechos de los interesados** : establecer una regulación más específica de los procedimientos a seguir para el ejercicio y la atención de los derechos de los interesados (plazos, documentación o

	información a aportar por el interesado, subsanación de solicitudes que carezcan de dichos requisitos, etc.) La AEPD dispone de un procedimiento de Tutela de Derechos, regulado en el Capítulo II del Título IX del RLOPD, que se caracteriza por no tener un fin sancionador. Consideramos igualmente conveniente que este procedimiento se regule en la nueva norma. **Regulación específica de las cesiones o comunicaciones de datos** es necesario que se regule de forma más específica esta cuestión, por ejemplo de forma semejante a lo recogido actualmente en el artículo 11 de la LOPD. **OTRAS CUESTIONES** **Validez de los contratos de encargo de tratamiento LOPD** se debe regular expresamente la validez de los contratos firmados conforme al artículo 12 de la LOPD con fecha anterior al 25 de mayo de 2018. **Validez consentimientos LOPD** (Considerando 171 del RGPD) es conveniente que se establezca expresamente la validez de estos consentimientos tácitos prestados legalmente, pues lo contrario podría implicar la vulneración del principio de irretroactividad de las normas. **Co-registro** el RLOPD (art. 57), y el el RGPD (art. 26) prevén la posibilidad de que existan 2 o más responsables de un mismo fichero o tratamiento de datos personales pero ninguna de las normas prevé la posibilidad de que a través de un mismo formulario se recaben datos para 2 o más responsables independientes, con distintas finalidades y usos, lo que sucede muy habitualmente en determinadas colaboraciones entre empresas (p.e. eventos, concursos, sorteos y otros productos o servicios creados en colaboración por diversas empresas) en los que el sector ha implantado una figura (la del co-registro) que no está desarrollada ni regulada claramente desde el punto de vista legal. A falta de regulación específica se aplican los mismos criterios y obligaciones que se aplicarían para varios ficheros o tratamientos independientes, pero convendría regularlo de forma legal. **Plazos expresados en semanas y meses** Consideramos pertinente que la nueva norma se pronuncie sobre si los plazos expresados en semanas se referirán a 7 días naturales o por si por el contrario se referirán a días hábiles. También consideramos necesaria la aclaración de si los plazos expresados en meses se computarán “de fecha a fecha”. **Resolución de conflictos entre normas extraterritoriales** El RGPD es una norma que prevé su aplicación de forma extraterritorial (arts. 3.2 y 3.3 del RGPD).Sin embargo, en su Considerando 115, rechaza la posibilidad de que se apliquen de forma extraterritorial otras leyes de protección de datos. Consideramos conveniente que se regule un mecanismo de auxilio o de ayuda por parte de las autoridades de protección de datos en la resolución de conflictos entre normas.
ANGECO Asociación Nacional de Entidades de Gestión de Cobro	que se mantenga pero amplíe a los Encargados de Tratamiento de Datos el procedimiento recogido en los artículos 153 a 156 del actual Reglamento de desarrollo de la vigente Ley Orgánica de Protección de Datos Personales para exonerar del Derecho de Información bajo determinadas prerrogativas y concesiones a los

	Responsables de Ficheros/Tratamiento
GOOGLE	interés legítimo estaría justificado,mejor principios que lista exhaustiva -mayor claridad en cuanto al alcance de la portabilidad de datos. -Tratamiento automatizado (Art. 22). sería deseable mantener la literalidad del precepto en la normativa española, teniendo presente el Art. 9 (2), que exige a los responsables del tratamiento el establecimiento de garantías adecuadas para ello.- "One Stop Shop"Tratándose de un mecanismo de nueva creación, creemos conveniente basar su adopción en la normativa española en las directrices que el Grupo de Trabajo del Artículo 29 viene trabajando en el ámbito europeo
FUNDACIÓN ESYS	**<u>Consentimiento</u>** - Las Empresas deberían poder obtener un consentimiento válido basado en sistemas de opt-in (consentimiento expreso) flexibles que garanticen el consentimiento inequívoco inicial del interesado mediante "una declaración o una clara acción afirmativa", pero sin necesidad de tener que hacer una re-validación,y no deberían estar obligadas a recoger un nuevo consentimiento cualificado a los interesados que ya otorgaron un consentimiento tácito válido bajo la LOPD, pues ello iría en contra de los principios de no retroactividad y de seguridad jurídica. - En cualquier caso, los tratamientos con fines de ejecución de un contrato o para el envío de información comercial sobre productos o servicios de la propia Empresa deberían poder seguir realizándose después del 25 de mayo de 2018 sin necesidad de recabar de los interesados el consentimiento cualificado que exige el Reglamento Europeo. **<u>Seudonimización y anonimización</u>** - aclarar qué técnicas de y anonimización son adecuadas y en qué consisten. - reconocer a los datos seudonimizados un status equiparable a los datos anonimizados cuando reúnan las suficientes garantías de irreversibilidad en la identificación de los interesados. **<u>Interés legítimo</u>** - aclarar qué tratamientos de datos personales quedarán cubiertos por el concepto del interés legítimo. - definir el término "fuente de acceso público" y aclarar si los ficheros de información sobre solvencia patrimonial y crédito, los ficheros con fines de publicidad y de prospección comercial, el uso del censo promocional y las denominadas "Listas Robinson" seguirán regulándose conforme a lo previsto en la LOPD y en el RPD. **<u>Big Data e Internet de las Cosas</u>** -Sería útil contar con algún documento de la AEPD donde, consultados los sectores interesados, se analicen las implicaciones legales derivadas del Big Data y el Internet de las Cosas con ejemplos claros de cuándo puede considerarse en qué entornos de este tipo se están tratando datos personales y cuándo no y, en el primer caso, qué

	requisitos deberán cumplirse para el tratamiento de los datos. **Derechos de los interesados** - La AEPD debería aprobar el contenido estándar del archivo que deba entregarse al interesado o, en su caso, al nuevo Responsable, cuando se ejerza el derecho a la portabilidad de los datos. También debería definir el formato y la forma de transmitirse este archivo al nuevo Responsable. - La AEPD debería aclarar cuándo, en el marco del ejercicio del derecho de oposición, una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, produce efectos jurídicos en el interesado o le afecta significativamente de modo similar. **Notificación de ficheros de datos** - modificar la LOPD y el RPD para derogar los artículos de estas normas que regulan la obligación de comunicar al Registro General de Protección de Datos los ficheros de datos personales, incluidos los ficheros de Videovigilancia. **Registros de las Actividades de Tratamientos** - publicar una Guía Interpretativa donde se aclaren los conceptos "riesgo para los derechos y libertades de los interesados" y "tratamiento no ocasional" de datos personales. También sería conveniente que se determinasen los "campos" que deberán tener los Registros de las Actividades de Tratamientos. **Evaluaciones de Impacto y Consultas Previas** - publicar una lista de los tratamientos que requerirán una Evaluación de Impacto o PIA (siglas en inglés de *Privacy Impact Assessment*) y de los que no, con una definición lo más clara posible de los conceptos "alto riesgo para los derechos y libertades de las personas", "evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado", "tratamiento a gran escala" y "observación sistemática a gran escala de una zona de acceso público. Sería muy útil la aprobación de un modelo de PIA europeo. **Comunicaciones de Violaciones de Seguridad de los datos personales** - aclarar si el procedimiento disponible en la sede electrónica de la AEPD para que los prestadores de servicios de comunicaciones electrónicas notifiquen Violaciones de Seguridad va a ser también aplicable a todas las Empresas que deban comunicar brechas de Seguridad conforme al Reglamento Europeo. Si no lo va a ser, la AEPD debería aprobar uno específico para todas las empresas deban comunicar violaciones de seguridad en virtud del Reglamento Europeo. Podría ser utilizable la norma CCN-STIC-817 publicada por el Centro Criptográfico Nacional para su uso por las Administraciones Públicas. - aclarar en qué casos puede decirse que es probable que una Violación de la Seguridad de los datos personales entrañe un "alto riesgo para los derechos y libertades de las personas físicas" a los efectos de comunicar la violación a los interesados afectados. -Cuando una brecha de Seguridad sea notificada a varias autoridades, organismos o administraciones en virtud de

	distintas normas, aquellos deberán actuar de manera coordinada para abordar el análisis y resolución del incidente de forma coherente, sin tomar decisiones que puedan ser contradictorias entre sí. **Regulación del estatuto jurídico del Delegado de Protección de Datos (DPO)** regular el estatuto jurídico del DPO con indicación de qué responsabilidades podría asumir, en su caso. **Transferencias Internacionales de Datos** aclarar cuáles serán las consecuencias que para las Empresas que transfieran datos personales a EE.UU., al amparo del nuevo acuerdo denominado Escudo de la Privacidad entre la Unión Europea y EE.UU., se derivarían de la eventual anulación de dicho acuerdo por el Tribunal de Justicia de la Unión Europea (TJUE), así como de la anulación por los tribunales nacionales o el TJUE de cualquier otra decisión o acto de una Autoridad Nacional de Control o de la Comisión Europea que haya dado cobertura legal a una transferencia internacional de datos. Las empresas afectadas no deberían quedar expuestas a sanciones como consecuencia de tal anulación, como tampoco los tribunales deberían otorgar indemnizaciones a los interesados si se demuestra que la Empresa en cuestión actuó de forma diligente y sobre la base del principio de confianza legítima en la legalidad y eficacia de los actos de la Administración. **Videovigilancia** revisar la Instrucción 1/2006 y precisar que los archivos temporales de imágenes de vídeo no son archivos de datos de carácter personal, y que sólo lo son aquellos archivos de grabaciones de vídeo que incluyan metadatos, que permitan correlacionar las imágenes con las identidades de las personas que aparecen en dichas grabaciones. **Medidas de Seguridad** - orientar a las Empresas sobre las medidas de Seguridad que tendrán que adoptar para cumplir con el Reglamento Europeo a partir de mayo de 2018, bien mediante la publicación de Directrices de la AEPD, bien mediante la aprobación de Códigos de Conducta o Mecanismos de Certificación que contengan las medidas de seguridad recomendadas para distintos sectores. Sería importante eliminar en cualquier caso la obligación de almacenar copias de respaldo, en aquellos casos que los datos no son útiles para el propietario de los mismos nada más que temporalmente (por ejemplo, los registros de accesos a un edificio). -A la hora de orientar a las empresas sobre cuáles deben ser esas medidas, el Ministerio de Justicia y la AEPD debería tener en cuenta que ya existe normativa sectorial y Normas internacionales y estándares consolidados certificables que definen las medidas de Seguridad aplicables en algunos ámbitos, por ejemplo, a los titulares o gestores de Infraestructuras Críticas, prestadores de servicios de comunicaciones electrónicas, operadores de servicios esenciales, proveedores de servicios digitales, etc. **Sanciones** - decidir si se mantienen las sanciones contempladas en la LOPD o se modifican o añaden nuevas. Además, deberá establecer, en su caso, las multas aplicables a las Administraciones y Órganos Públicos, y el régimen transitorio de los

	procedimientos sancionadores iniciados conforme a la LOPD antes del 25 de mayo de 2018.
SIGACUS GESTIÓN S.L.	, es muy importante que NO se suprima la obligatoriedad de inscripción por parte de las empresas de sus ficheros o tratamientos de datos personales en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos. Por una parte, el mencionado Registro, que como Ud. sabe es de acceso público y gratuito a través del sitio web de la Agencia, es crucial para que los ciudadanos puedan consultar qué empresas y entidades realizan tratamientos de datos y cómo poder ejercer ante ellas sus derechos fundamentales de acceso, rectificación, cancelación y oposición, así como la tutela de derechos ante la propia Agencia. Por otra, la obligatoriedad de inscripción de ficheros y tratamientos de datos ha supuesto la vía de conocimiento y difusión principal de esta importantísima normativa en la mayoría de las empresas, tanto grandes como medianas y pequeñas. Su supresión dañaría enormemente la difusión de la normativa, y como consecuencia el cumplimiento de la misma y la propia defensa del derecho fundamental a la protección de datos personales y a la privacidad. Por todo ello solicito que se mantenga el Registro General de Protección de Datos y la obligatoriedad de inscripción de ficheros y tratamientos de datos en él.
CONSEJO GENERAL DE FARMACÉUTICOS	-cabría si así se estima, recoger en la Ley Orgánica que se tramite el supuesto planteado o bien contemplar la situación descrita referida al ámbito de la atención farmacéutica en la dispensación de medicamentos, bien en el Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de Garantías y uso racional de los medicamentos y productos sanitarios, en su artículo 86 de las oficinas de farmacia, o bien con carácter general y para todo el ámbito sanitario, incluyendo el farmacéutico, mediante una modificación expresa en la Ley 41/0002, para recoger la posibilidad de que en el ámbito sanitario y farmacéutico, el derecho a la información y el consentimiento informado para pacientes impedidos por su estado -derivado situaciones de determinadas de enfermedades como, alzhéimer, demencia senil, discapacidad psicológica grave, etc.-, pueda realizarse por personas vinculadas a él que por razones familiares o de hecho - en la nueva normativa de protección de datos que se elabore en desarrollo del Reglamento Europeo, se debería contemplar expresamente en alguno de los artículos de la Ley Orgánica que se tramite el régimen jurídico y la peculiar naturaleza de las Organizaciones Colegiales Profesionales para clarificar aquellos extremos a los que por razón de su naturaleza dual (pública y privada) se encuentran sometidas. Podría realizarse, si así se estima oportuno, equiparando

	en concreto con la Administración Públicas aquellos tratamientos de datos que se realizan en el ejercicio de potestades públicas, con arreglo a las funciones que establece la Ley de Colegios Profesionales, en cuanto a los datos de los profesionales colegiados, y procedimientos sancionadores así como en desarrollo de otras funciones que por estar en normativas sectoriales así lo determinan.
AMCHAMUE	-las funciones del Delegado de Protección de Datos cuando se traten de sistemas de datos corporativos grandes deberán estar realizadas por un Ingeniero en Informática o Máster en Ingeniería en Informática. Se diferencian por tanto las organizaciones de menor tamaño y con tratamientos de poca complejidad de las organizaciones de gran tamaño y con tratamientos de gran complejidad las cuales requerirán un servicio más profesional y mayor capacidad técnica del Delegado de Protección de Datos. -El Representante del responsable o el encargado del tratamiento no establecido en la Unión que esté tratando datos personales de interesados que residan en la Unión Europea deberá tener la suficiente capacidad técnica y profesional garantizada con la figura de un Ingeniero en Informática colegiado. -Habilitar por Ley a los COLEGIOS PROFESIONALES DE INGENIEROS EN INFORMÁTICA DEL ESTADO ESPAÑOL como certificadores de los esquemas previstos por el RGPD. -Habilitar por Ley a los COLEGIOS PROFESIONALES DE INGENIEROS EN INFORMÁTICA DEL ESTADO ESPAÑOL como autoridad de supervisión auxiliar en el ámbito del RGPD. De esta forma los COLEGIOS DE INGENIEROS EN INFORMÁTICA DEL ESTADO ESPAÑOL participarán en la publicidad del nuevo RGPD, aclararán dudas a los ciudadanos, formarán a profesionales especialistas en la Protección de Datos, colaborarán en el desarrollo de herramientas que faciliten la identificación y valoración de riesgos y en recomendaciones sobre la aplicación de medidas. -Las empresas deben adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece, de ahí que se permita avisar a los Responsables de Ficheros de vulnerabilidades detectadas, pero visto las sentencias que se han producido en nuestro país en base a estos avisos,en las cuales se termina denunciando a quien de buena fe a avisado al Responsable del Tratamiento, se hace necesario depositar la confianza en una autoridad independiente, como son los COLEGIOS PROFESIONALES DE

	INGENIEROS EN INFORMÁTICA DEL ESTADO ESPAÑOL como autoridad de supervisión auxiliar, donde se preste el servicio de recogida de vulnerabilidades de sistemas de datos, a fin de que se puedan concretar y avisar a sus Responsables de Ficheros con un informe técnico de dicha vulnerabilidad. Según (85) del RGPD "Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas [...] Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación [...]" Por ello, se hace necesaria la mediación de los profesionales Ingenieros en Informática para evaluar las falsas amenazas y discernir los problemas técnicos de los sistemas.