AYUNTAMIENTO DE PAMPLONA
I.SEGURA@PAMPLONA.ES

Registro de Entrada: O00007128e2100001557

En relación con su consulta, referente a si es "imprescindible que las empresas licitadoras cumplen con la normativa Une 15713 –DIN 66399 y se encuentren certificadas o en caso contrario qué medidas concretas es necesario exigir que cumplan los licitadores para garantizar la correcta destrucción de la documentación"; pueden consultar la información disponible al respecto en esta dirección:

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

En estas Directrices sobre notificación de violación de datos personales según el Reglamento 2016/679 (wp250rev.01), del Comité Europeo de Protección de Datos (CEPD o EDPB por sus siglas en inglés), reseñado al comienzo, podemos leer como cuestión preliminar lo siguiente:

"El concepto de «destrucción» de los datos personales debe estar muy claro: es cuando los datos ya no existen, o ya no existen en una forma que sea de utilidad para el responsable del tratamiento. El concepto de «daño» también debe estar relativamente claro: cuando los datos personales han sido alterados, corrompidos o dejan de estar completos. La «pérdida» de datos personales debe interpretarse en el sentido de que los datos pueden seguir existiendo, pero el responsable del tratamiento ha perdido el control o el acceso a ellos, o ya no obran en su poder. Por último, el tratamiento no autorizado o ilícito puede incluir la divulgación de datos personales a (o el acceso por parte de) destinatarios que no están autorizados a recibir (o acceder a) los datos, o cualquier otra forma de tratamiento que vulnere el RGPD".

El artículo 32 del RGPD, "Seguridad del tratamiento", establece en su apartado 1 lo siguiente por otro lado:

"Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

Código Seguro De Verificación:	APDPFA30C9B8B1FDF23D8610-99518	Fecha	09/02/2021
Normativa	Este documento incorpora la firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior		
Firmado Por	Jefe de Servicio - Lourdes Hernández Crespo		
Url De Verificación	https://sedeagpd.gob.es	Página	1/4

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento".

Por otra parte, debe tenerse en cuenta que es el responsable del tratamiento en cuestión el que elige al correspondiente encargado y siempre que éste le ofrezca "garantías suficientes" en el tratamiento con medidas técnicas y organizativas apropiadas, cumpliendo con el RGPD y garantizando la protección de los derechos de los interesados. Es por ello conveniente que en la redacción de las correspondientes cláusulas que vayan a regir el encargo se regule este tema, pues una vez asumidas por ambas partes, quedan éstos vinculados, bajo la responsabilidad del responsable, que determina los fines y medios del tratamiento y dicta las oportunas instrucciones a seguir en caso de que se produzca un incidente de seguridad. En este sentido, el hecho de que aquél que preste servicios a un responsable, que requiera un determinado tratamiento (aquí, "destrucción", ver artículo 4.2 del RGPD), podrá tener en consideración el cumplimiento de estándares de actuación como el que ustedes mencionan en su consulta, lo que viene a ser un plus en tal obligación a la hora de la elección del encargado que ofrezca garantías de seguridad desde la perspectiva la normativa de protección de datos personales.

En este sentido, como bien saben, la DIN 6399 fue desarrollada en Alemania por el Deutsches Institut für Normung o Instituto Alemán para la Normalización que se dedica a elaborar los estándares para asegurar la calidad en los servicios prestados en diversos sectores. Sus siglas DIN corresponden a Das Ist Norm (Esto es norma). En particular la DIN 66399 se ocupa de la distinas clases de protección en la destrucción de documentos. Por otra parte, una empresa certificada bajo la norma UNE 15713 vendría a dar garantías al responsable del compromiso de la utilización de medios para que la destrucción efectiva se produzca de forma segura.

La regulación de la relación entre el responsable y el encargado del tratamiento, de acuerdo con lo establecido en el artículo 28 del RGPD, debe establecerse en consecuencia a través de ese contrato (o de un acto jurídico similar) y debe constar por escrito, inclusive en formato electrónico, a efectos de acreditar tal vinculación a lo pactado.

Resaltar que, en todo caso, el apartado 3.f) de este artículo 28 establece que el encargado del tratamiento "ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado". Ello en el contexto de tomar "todas las medidas necesarias" de seguridad de conformidad del artículo 32 (apartado 3.c del artículo 28). Cuestiones que en particular deberán quedar estipuladas en el ya mencionado contrato o acto jurídico, de obligado cumplimiento para el encargado.

El artículo 28, "Obligaciones generales del responsable y encargado del tratamiento", de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establece en este sentido en su apartado 1 que:

Código Seguro De Verificación:	APDPFA30C9B8B1FDF23D8610-99518	Fecha	09/02/2021
Normativa	Este documento incorpora la firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior		
Firmado Por	Jefe de Servicio - Lourdes Hernández Crespo		
Url De Verificación	https://sedeagpd.gob.es	Página	2/4

"Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable".

Y para la adopción de estas medidas deberán tener en cuenta, en particular, "los mayores riesgos" que podrían producirse "Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados" (apartado 2.a).

No olvidar en definitiva que es el responsable del tratamiento no obstante el que responde del incumplimiento del RGPD, salvo que el propio encargado actúe por su cuenta, al margen de las instrucciones recibidas, en cuyo caso habrá que estar a lo establecido en los artículos 28.10 y 29 del RGPD.

En las ya citadas Directrices sobre incidencias en la seguridad de datos personales podemos leer lo siguiente:

"El responsable del tratamiento también debe haber establecido acuerdos con los encargados del tratamiento a los que recurra, los cuales tienen a su vez la obligación de notificar la violación al responsable del tratamiento del caso (véase a continuación).

Si bien corresponde a los responsables y a los encargados del tratamiento adoptar las medidas adecuadas para poder prevenir, reaccionar y hacer frente a una violación, en todos los casos deben adoptarse algunas medidas prácticas.

• La información relativa a todos los sucesos relacionados con la seguridad debe dirigirse a la persona o personas responsables de hacer frente a los incidentes, determinar la existencia de una violación y evaluar el riesgo.

• Debe evaluarse el riesgo para las personas derivado de una violación (probabilidad de que no haya riesgo, de que haya riesgo o riesgo alto), y se debe informar a los departamentos pertinentes de la organización.

• En caso necesario debe hacerse la notificación a la autoridad de control y, en su caso, la comunicación de la violación a las personas afectadas.

• Al mismo tiempo, el responsable del tratamiento debe actuar para contener y recuperar la violación.

• La documentación de la violación debe realizarse a medida que esta se desarrolla.

Código Seguro De Verificación:	APDPFA30C9B8B1FDF23D8610-99518	Fecha	09/02/2021
Normativa	Este documento incorpora la firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior		
Firmado Por	Jefe de Servicio - Lourdes Hernández Crespo		
Url De Verificación	https://sedeagpd.gob.es	Página	3/4

Por consiguiente, debe quedar claro que el responsable del tratamiento está obligado a actuar a partir de cualquier alerta inicial y a determinar si se ha producido o no una violación. Este breve período permite que se realicen algunas investigaciones y que el responsable del tratamiento reúna pruebas y otros detalles pertinentes. No obstante, una vez que el responsable del tratamiento haya establecido con un grado razonable de certeza que se ha producido una violación, si se cumplen las condiciones del artículo 33, apartado 1, deberá notificarlo a las autoridades de control sin dilación indebida y, de ser posible, en un plazo máximo de setenta y dos horas. Si un responsable del tratamiento no actúa de manera rápida y resulta evidente que se ha producido una violación, esto podría considerarse una falta de notificación de conformidad con el artículo 33.

El artículo 32 deja claro que el responsable y el encargado del tratamiento deben disponer de las medidas técnicas y organizativas adecuadas para garantizar un nivel adecuado de seguridad de los datos personales: la capacidad para detectar, abordar y notificar una violación en tiempo oportuno debe considerarse un elemento esencial de estas medidas".

Insistir en que, por aplicación de los principios de responsabilidad proactiva y rendición de cuentas, se documentará todo lo referente a la violación de seguridad y se adoptarán por parte del responsable las medidas necesarias "para poner remedio" a lo ocurrido, sobre todo, la justificación documental de una posible dilación, en especial, a la hora de determinar si ésta es "indebida" o no. En el presente caso, evaluar si no ha existido una destrucción total y efectiva de la documentación en cuestión, que permita acceder a datos personales en ellos contenidos ("cuando los datos ya no existen", de forma que no puedan ser objeto de un tratamiento ulterior por imposibilidad material), más si son de categoría especial.

Por útlimo, recordar que el delegado de protección de datos tendrá como función "supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes" (artículo 39.1.b del RGPD); en sintonía en el presente caso concreto con lo que disponga la legislación sectorial de aplicación en materia de contratación pública.

Atentamente.

Código Seguro De Verificación:	APDPFA30C9B8B1FDF23D8610-99518	Fecha	09/02/2021
Normativa	Este documento incorpora la firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior		
Firmado Por	Jefe de Servicio - Lourdes Hernández Crespo		
Url De Verificación	https://sedeagpd.gob.es	Página	4/4