ANEXO 19

ESPECIFICACIÓN TÉCNICA

REQUISITOS APLICABLES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

1. OBJETO.

El objetivo de este anexo es definir los requisitos aplicables en materia de protección de datos personales en el proceso de elaboración de las especificaciones técnicas, con la finalidad de asegurar que todas las actividades contratadas por ANAV cumplen la legislación sobre protección de datos personas y garantizar su adecuación al Reglamento General de Protección de Datos (RGPD) .

2. APLICABILIDAD.

A todos los contratos que vinculen datos personales.

3. REFERENCIAS.

- PG-0.09 Protección de datos personales Rev.2
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

4. DEFINICIONES Y SIGLAS.

4.1 Definiciones.

- **Datos de carácter personal:** toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

- **Encargado del tratamiento o Encargado:** la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

- **Responsable de información del tratamiento:** la persona física, nombrada por el Responsable del Tratamiento, que tiene asignadas formalmente la función de responsable de establecer los requisitos de acceso, tratamiento y conservación de la información relacionada con un tratamiento de datos de carácter personal.

- **Tratamiento de datos:** cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración,

conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

4.2 Siglas.

- **ANAV:** Asociación Nuclear Ascó Vandellòs II AIE
- **UO:** Unidad organizativa

5. CONTRATOS CON ENCARGADOS DE TRATAMIENTO

No se podrá encargar un tratamiento a un tercero si previamente no se realiza un contrato entre las partes donde se incluya expresamente información sobre las obligaciones relacionadas con los datos personales.

En ningún caso un encargado de tratamiento podrá subcontratar el servicio encomendado, ni en su totalidad ni en parte, sin la autorización previa de ANAV. Si se solicita una subcontratación, ANAV analizará a la tercera empresa como si fuera su propio encargado de tratamiento y obligará a aplicar las clausulas sobre protección de datos del contrato con el encargado de tratamiento a la empresa subcontratista.

Todos los contratos donde se vinculen tratamientos de datos personales incluirán cláusulas contractuales relativas a la protección de los datos personales que establecerán estos contenidos mínimos:

- el objeto, la duración, la naturaleza y la finalidad del tratamiento
- el tipo de datos personales y categorías de interesados
- las obligaciones y derechos del responsable
- Obligaciones del encargado:
  - Tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable,
  - Garantía de confidencialidad
  - Aplicar todas las medidas necesarias para garantizar la seguridad de los datos
  - Condiciones para la subcontratación a un tercero
  - Colaboración con el responsable para facilitar el ejercicio de los derechos de los interesados
  - Colaborar con el responsable para el mantenimiento de la seguridad de los datos personales.
  - Medidas de devolución de los datos a finalización del servicio contratado
  - Poner a disposición de ANAV toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el contrato, así como la realización de auditorías por parte de ANAV o de otro auditor autorizado por ANAV.

ANAV, a través de la Unidad de Aprovisionamientos, cuenta con cláusulas tipo de contratación de un tratamiento que garantizan el cumplimiento de los requisitos legales y por ello se deben incorporar a todos los contratos que vinculen datos personales:

- Condiciones generales de contratación de ANAV
- Condiciones particulares en el tratamiento de datos de carácter personal por un encargado de tratamiento. Las condiciones particulares en el tratamiento de datos de carácter personal por un encargado de tratamiento se encuentran en el **Anexo VIII del PG-0.09**. Dicho anexo lo ha de cumplimentar la propia UO que contrata el servicio, indicando el detalle de los diferentes tratamientos a realizar:
    - Operaciones de tratamientos de datos
    - Información que la UO pone a disposición del encargado de tratamiento: categorías interesado, categorías de datos

Si el prestador de servicio no tiene la necesidad de acceder a los datos personales, se deberá recoger expresamente en el contrato la prohibición del acceso y la obligación de secreto, además de adoptar las medidas encaminadas a impedir el acceso a los datos contenidos en soportes o documentos.

6. ELECCIÓN DE ENCARGADOS DE TRATAMIENTO CON GARANTIAS

6.1 Evaluación inicial

ANAV, con el fin de garantizar la adecuación de proveedores de servicios relacionados con los datos personales, realiza la elección de los encargados de tratamientos con garantías donde:

- Se analiza el cumplimiento en materia de protección de datos.
- Se realiza un seguimiento periódico que garantice el mantenimiento de los niveles exigidos respecto a la seguridad.

Antes de la contratación con un nuevo proveedor como encargado de tratamiento en materia de datos personales, éste debe contar con una evaluación positiva. **Esta evaluación se realizará a aquellos encargados de tratamientos relacionados con tratamientos de datos de carácter personal de riesgo alto** y se analizará en función del riesgo asociado al tratamiento contratado por el Responsable de Seguridad en colaboración con la Unidad de Aprovisionamiento de ANAV y el Responsable de Información del Tratamiento de datos personales.

La evaluación se realizará para aquellos proveedores que son encargados de tratamiento relacionados con las actividades de tratamiento de ANAV y que se encuentran identificados en el ANEXO II.II: REGISTRO DE TRATAMIENTOS DE DATOS PERSONALES y que están relacionados con tratamientos de datos de carácter personal de riesgo alto.

El Responsable de Seguridad mantendrá un registro donde se reflejen los resultados de las evaluaciones a disposición de las Unidades Organizativas de ANAV.

Para realizar la evaluación, ANAV se ayudará de la plantilla de evaluación denominada ‘Compromiso de cumplimiento de un encargado de tratamiento en materia de protección de datos personales’ (Anexo IX del PG-0.09) que la Unidad de Aprovisionamiento enviará

al proveedor (al menos, a aquellos encargados de tratamientos relacionados con tratamientos de datos de carácter personal de riesgo alto) para su cumplimentación, y se lo comunicará al Responsable de Seguridad, quien se encarga de su evaluación, según los siguientes criterios.

Los criterios establecidos para la evaluación son:

1. En el caso que el proveedor cuente con una certificación de cumplimiento en materia de protección de datos confiable, la evaluación puede basarse en dicho certificado sin necesidad de otras revisiones añadidas. Se verificará que dicho certificado incluye en su alcance el tratamiento objeto de contrato.
2. En aquellos contratos relacionados con tratamientos de nivel de riesgo alto que no cuenten con una certificación, ANAV podrá realizar una auditoría de cumplimiento legal y de implantación de medidas de seguridad. El coste de esta auditoría se acordará con el encargado de tratamiento previamente.
3. En otro caso, se valorará la siguiente documentación aportada por el contratista:
   a. Informes de auditoría en protección de datos
   b. Informes de auditoría sobre seguridad de la información
   c. Certificaciones en seguridad de la información.
   d. Políticas, normas y procedimientos en materia de protección de datos y seguridad e la información.

   Esta documentación será analizada para comprobar si las medidas implementadas por el encargado de tratamiento garantizan los niveles de seguridad exigidos por ANAV.

4. En el caso que el proveedor no cuente con documentación que avale el nivel de seguridad exigido, ANAV remitirá la plantilla de autoevaluación (‘Compromiso de cumplimiento de un encargado de tratamiento en materia de protección de datos personales’) al proveedor.

A la vista de la información anterior, se podrá tomar las siguientes decisiones:

1. Aceptar al proveedor como encargado de tratamiento y comenzar la evaluación periódica.
2. Aceptar al proveedor como encargado de tratamiento provisionalmente (evaluación positiva temporal). Se le solicitarán una serie de medidas correctoras definiendo un plan de acción: objetivos, plazos, responsables y recursos. Una vez cumplido el plazo se revisará la aplicación de dichas medidas, aceptando al proveedor (pto 1) o denegando su aprobación (pto. 3).
3. Denegar al proveedor la condición de encargado de tratamiento. Esto supone la imposibilidad de obtener o mantener un contrato a través del cual realice un tratamiento de datos personales en nombre de ANAV.

Adicionalmente y de forma periódica se volverá a enviar, para el mantenimiento de la evaluación, a cada encargado de tratamiento siguiendo los criterios y las periodicidades establecidas en el apartado 6.4.2 del PG-0.09 Rev 2.