RESOLUCIÓN DE LA DIRECCIÓN DE LA AGENCIA TRIBUTARIA DE ANDALUCÍA PARA FACILITAR LA IMPLEMENTACIÓN DE LA PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO.

La Resolución de 6 de julio de 2020, de la Agencia Tributaria de Andalucía, por la que se aprueba la Política de Seguridad de la Información de esta Agencia, así como la estructura organizativa responsable de su ejecución, concibe la protección de datos de carácter personal como uno de los "(...) principios básicos de la Política de Seguridad de la Información y que inspiran las actuaciones de la Agencia". Desde esta perspectiva, la protección de datos debe estar en la base de todas las acciones que se emprendan, no como algo accesorio sino como un pilar de la prestación de servicios a los ciudadanos, debiendo adoptarse una actitud consciente, diligente y proactiva.

La Agencia viene trabajando de modo intensivo en diversos marcos de actuación en esta materia: organizativo, operacional y de medidas de protección del Esquema Nacional de Seguridad. Con el propósito de actuar en clave de mejora continua para favorecer el cumplimiento de la normativa de protección de datos, se incorpora a la planificación estratégica de la Agencia diversas propuestas de actuación realizadas por la Inspección General de los Servicios en distintas áreas de trabajo.

Dentro del marco de medidas de protección, y desde la perspectiva de la gestión del personal la Agencia viene realizando numerosas actuaciones de diversa naturaleza, entre las que destacan la elaboración de un Manual de bienvenida – Nociones básicas sobre el uso seguro de las TIC- y la organización de un conjunto de acciones de concienciación, que incluye un catálogo amplio de actividades con distinto alcance: publicación de boletines de seguridad, boletines internos de noticias que incluye un capítulo monográfico para la difusión de comunicaciones con fines de sensibilización en materia de seguridad de la información y protección de datos, sesiones informativas de difusión específicas en esta materia, mensajes emergentes de concienciación durante el acceso al Sistema Unificado de Recursos SUR o simulacros de incidente de seguridad.

La seguridad de la información y la protección de datos es, por tanto, un campo de actuación estratégico, que informa y orienta toda la actividad que desarrolla la organización en todas sus áreas de trabajo. A tal efecto, la implicación del personal resulta esencial no solo para el cumplimiento escrupuloso de la normativa de seguridad y protección de datos, sino para el establecimiento de buenas prácticas inherentes al buen gobierno y a la reputación corporativa de la organización.

En este escenario el Plan de Actuaciones en materia de Seguridad de la Información y Protección de Datos 2022, aprobado por el Comité de Seguridad TIC y Seguridad Interior en sesión de 4 de febrero de 2022, identifica diferentes marcos de actuación: protección de datos desde el diseño y por defecto, responsabilidad proactiva, implementación y seguimiento de la protección de datos, formación y concienciación, así como en la detección, gestión y registro de brechas que afecten a datos personales.

Para contribuir a que la organización y las personas que forman parte de la Agencia alcancen con éxito los objetivos enunciados con anterioridad, la Agencia dispone de los siguientes órganos y unidades administrativas:

- Comité de Seguridad TIC y Seguridad Interior.
- Responsable de Seguridad TIC.
- Responsable de la Información.
- Responsable del Sistema.
- Grupo de Trabajo Permanente.
- Comisión Técnica de Seguridad Funcional.
- Delegado de Protección de Datos.

Particularmente, la figura del Delegado de Protección de Datos resulta decisiva en la gestión de la seguridad de la información y protección de datos, desempeñando un papel esencial en tareas de asesoramiento y supervisión en esta materia y en la generación de recursos informativos y en la difusión de buenas prácticas que contribuyan, en clave de mejora continua, al cumplimiento proactivo de la normativa de protección de datos. Por tanto, el desarrollo de las tareas de asesoramiento y supervisión por parte del Delegado de Protección de Datos deben llevarse a cabo en un marco ordenado, sistemático y eficiente, en las siguientes áreas de trabajo:

- Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.

- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.

- Diseño e implantación de políticas de protección de datos.

- Auditoría de protección de datos.

- La gestión de los registros de actividades de tratamiento.

- Análisis de riesgo de los tratamientos realizados.

- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.

- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.

- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.

- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.

- Realización de evaluaciones de impacto sobre la protección de datos.

- Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

En el contexto descrito, se hace necesario establecer procedimientos de actuación que favorezcan el desarrollo de estas tareas por el Delegado de Protección de Datos al considerarse que son estratégicas para el desempeño ordinario de la actividad de la Agencia.

Sobre la base de cuanto antecede, teniendo en cuenta la actitud consciente, diligente y proactiva de la Dirección de la Agencia Tributaria de Andalucía como responsable del tratamiento, con arreglo a la Resolución de 6 de julio de 2020, de la Agencia Tributaria de Andalucía, por la que se aprueba la Política de Seguridad de la Información de esta Agencia, así como la estructura organizativa responsable de su ejecución (modificada por Resolución de 30 de junio de 2021, de la Agencia Tributaria de Andalucía, por la que se modifica el Anexo «Documento de Política de Seguridad TIC»), se dictan las siguientes instrucciones:

Primera. Objeto y ámbito de aplicación.

1. El objeto de la presente instrucción es establecer el procedimiento para implementar la protección de datos desde el diseño y por defecto. A través de este procedimiento se pretende disponer de un cauce específico para implementar la protección de datos desde el diseño y por defecto en la Agencia con la finalidad de identificar las técnicas y medidas organizativas que resultan apropiadas para

incorporar la protección de datos desde el diseño y por defecto, entre otras, la minimización, la pseudonimización o la limitación de la finalidad.

2. La instrucción se aplicará a:

a) Los órganos y unidades centrales y territoriales de la Agencia, en todos sus sistemas de información, y al personal destinado en dichos órganos y unidades.

b) El personal de otros organismos o entidades que, en virtud de norma jurídica, acuerdo o convenio, realicen tratamientos por encargo de la Agencia o tengan acceso a los sistemas de información de la Consejería competente en materia de Hacienda, puestos a disposición de la Agencia.

La resolución se aplicará en el marco del acuerdo de nivel de servicios con la Agencia Digital de Andalucía y de los instrumentos de planificación de la Agencia(contrato de gestión, plan de acción anual,...), e incluirá las infraestructuras de soporte para la actividad relativa a las tecnologías de la información y comunicación de la Agencia, servidores, centro de respaldo y almacenamiento, entorno de virtualización, gestión de portales, licencias y las necesarias medidas de seguridad, con las que se asegura el funcionamiento y custodia de la información derivada de la gestión tributaria, aprovechando las economías de escala de la integración en el conjunto de la Consejería competente en materia de Hacienda.

Segunda. Procedimiento para implementar la protección de datos desde el diseño y por defecto.

1. Con el propósito de facilitar el conocimiento y la participación del Delegado de Protección de Datos desde las fases tempranas en la planificación, diseño, desarrollo y ensayo de todas las funcionalidades, productos y servicios relacionados con el tratamiento de datos personales sensibles para la privacidad de la organización, los órganos y unidades de la Agencia competentes por razón de la materia remitirán una comunicación informativa al Delegado de Protección de Datos de las actuaciones que se propongan realizar en relación con los sistemas de tecnologías de la información que soportan el tratamiento de los datos, los procesos y las prácticas de aplicación de los tributos relacionados y el diseño físico y lógico de los canales de comunicación utilizados. A tal efecto, se remitirá comunicación informativa al Delegado de Protección de Datos con motivo de la realización de las siguientes actuaciones:

   - El borrador de documentos de planificación estratégica y operativa comprensivos de las actividades a realizar durante el ejercicio.

   - El borrador de documento de planificación de la formación que se prevé impartir por la Agencia cada año.

   - El borrador de la programación de las acciones de concienciación prevista en materia de seguridad y protección de datos.

   - El borrador de cualquier proyecto normativo impulsado por la Agencia o por un tercero que pudiera tener incidencia en materia de seguridad de la información y protección de datos.

- Los proyectos de normas y procedimientos de seguridad de la información y protección de datos de la Agencia.

- La planificación de nuevos desarrollos y funcionalidades que se prevean realizar cada año.

- Los proyectos de acuerdos, contratos o convenios de colaboración con terceros.

- Los borradores de formularios, en papel o electrónicos, así como de cualquier modelo de recogida de datos de los contribuyentes.

- Las declaraciones sobre privacidad y protección de datos en sitios y páginas web de personal.

- Así como el desarrollo de cualquier otra actuación relacionada con el tratamiento de datos personales.

2. Las comunicaciones informativas comprenderán, al menos, los siguientes extremos:

   - Breve descripción de la actuación que se propone realizar, la finalidad y objetivos previstos.

   - Calendario aproximado de implantación, puesta en funcionamiento o de ejecución de la actividad programada.

   - Cuando en el proceso de planificación, diseño, desarrollo y ejecución de la actividad intervengan diversos órganos, ya sea con carácter facultativo o preceptivo, se concretará el calendario previsto de intervención de cada órgano.

   Las comunicaciones informativas se acompañarán de los documentos que den soporte a las actuaciones anteriores, así como cualquier otro antecedente que se estime relevante para una mejor comprensión de las actuaciones que se propone realizar.

3. Las comunicaciones informativas y la documentación complementaria que la acompañe se remitirán por bandeja a la cuenta del Delegado de Protección de Datos.

4. La participación del Delegado de Protección de Datos en el Comité de Seguridad TIC y Seguridad Interior, el Grupo de Trabajo Permanente o la Comisión Técnica de Seguridad Funcional, no dispensará de la obligatoriedad de remitir la comunicación informativa prevista en esta instrucción.

EL DIRECTOR