POLITICA DE PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC
2024.11.04 09:17:34 +01'00'

Contenido

1. Información de control.

Resumen

TIPO	Política
ÁMBITO	Privacidad, Seguridad
TÍTULO	Política de privacidad desde el diseño y por defecto

Histórico de versiones

VERSIÓN	FECHA	REALIZADO POR	CAMBIOS
1.0	22/02/2024	Servicio Responsable Seguridad Delegada de Protección de Datos	

Control de aprobaciones

VERSIÓN	PRESENTADO	REVISIÓN	APROBACIÓN
1.0	Servicio Responsable Seguridad Delegada de Protección de Datos		Comité de Seguridad

1. Introducción

La protección de datos personales es una normativa que obliga a todas las organizaciones a adoptar una serie de medidas tendentes a garantizar la seguridad, la integridad y la confidencialidad, así como el correcto acceso, tratamiento, cesión, almacenamiento y eliminación, de los datos personales obrantes en Ziurtapen eta Zerbitzu Enpresa–Empresa de Certificación y Servicios, Izenpe, S.A. (en adelante, «Izenpe»).

El vigente Reglamento General Europeo de Protección de Datos, de 27 de abril de 2016 (en adelante, «RGPD») la normativa nacional sobre protección de datos personales y otra legislación que pueda resultar de aplicación, refieren la necesidad de implementar medidas de seguridad en esta materia, anticipándose a los nuevos requerimientos tecnológicos que precisan las organizaciones modernas y señalando la dirección a seguir por las organizaciones que tratan datos personales.

La necesidad de conectar el principio de responsabilidad proactiva (*accountabily*), con los instrumentos que favorecen su implementación, propician el exigible principio de Privacidad desde el Diseño (*Privacy by Design*), así como el uso de otros instrumentos como por ejemplo, la evaluación de impacto, conocida por su denominación inglesa: *Privacy Impact Assessment* o PIA (que son objeto de otro procedimiento específico sobre esta materia).

Según indica S. Garre Gui1, la privacidad por diseño y por defecto, así como el uso de evaluaciones de impacto, se desprenden de metodologías propias de ámbitos tecnológicos, lo que permite evaluar el impacto en la privacidad de cualquier iniciativa que implique tratamiento de datos personales, especialmente en los estados iniciales de la concepción, de forma que se puedan adoptar las medidas necesarias para evitar o reducir posibles consecuencias que pudieran afectar o comprometer los datos personales obrantes en Izenpe.

Conviene señalar que, desde un punto de vista de reducción de costes económicos, resulta mucho más útil incorporar metodología de supervisión desde la concepción de la actividad, ya sea esta una herramienta automatizada, una aplicación informática, un programa de actividades o de cualquier otra índole, que vaya a tratar datos personales, que valorar después de concebida e incluso de realizada, los inconvenientes que presenta desde un punto de vista de legalidad y tener que rehacerla.

Al respecto, la Agencia Española de Protección de Datos señala que «la información personal adquiere cada vez un mayor valor económico y, por ello, resulta imprescindible complementar los planteamientos tradicionales con nuevos enfoques proactivos que contribuyan a respetar los derechos de las personas y a fortalecer la confianza de los clientes y usuarios».

Ello no implica en modo alguno que se haya de abandonar el enfoque basado en la exigencia de cumplimiento de las disposiciones legales, sino que para garantizar este cumplimiento se hace cada vez más necesaria una disposición diligente, un compromiso responsable para evitar o minimizar los riesgos antes de que estos se materialicen.

En la línea de fortalecer la responsabilidad proactiva en Izenpe, resultan especialmente útiles enfoques como el de la Privacidad desde el Diseño, que propugna que las cuestiones de

[1] S. Garre Gui, *Introducción a la seguridad de la información*. Ed. Fundación UOC, Barcelona, 2006.

protección de datos y privacidad se tomen en consideración desde la fase inicial, desde el momento mismo del diseño de un producto o servicio.

Con ello se consigue no solo una mayor eficacia en la protección de los derechos de los afectados, sino también evitar algo que sucede con demasiada frecuencia: la reconvención a posteriori de la norma a la tecnología de tal forma que, una vez que esta ha sido desarrollada o implantada, se aprecia su irregularidad y ello lleva consigo altos costes para su rediseño y adaptación (Guía para la Evaluación de Impacto en protección de datos personales de la Agencia Española de Protección de Datos).

2. Objetivo.

Esta política tiene por objeto establecer las pautas de actuación para evaluar el impacto en la privacidad y el tratamiento de datos personales, ante cualquier iniciativa que incluya dicho tratamiento, especialmente en los estados iniciales de la concepción, de forma que se puedan adoptar las medidas necesarias para evitar o reducir posibles consecuencias que pudieran afectar o comprometer los datos personales obrantes en Izenpe.

Esta política complementa todas las medidas de seguridad y cumplimientos normativas que están implementados en Izenpe y que continúan con plena vigencia.

3. Ámbito de actuación y alcance.

La política se aplica a todo Izenpe y alcanza todos sus ámbitos. De forma especial, debe ser tenido en cuenta por todos los responsables de departamento y observado ante cualquier iniciativa interna o externa, de realizar acciones o proyectos para diseñar un proceso de cualquier índole, prestación de servicio, productos, programas o soportes informáticos, dispositivos, *app* o cualquier iniciativa análoga, que conlleve tratamiento de datos personales.

4. Principios de aplicación de la política y personal implicado.

La presente política se sustenta en unos principios orientados a garantizar la seguridad, integridad y confidencialidad de la información de carácter personal obrante en Izenpe, que deben estar presentes en los momentos de gestión de la iniciativa que se pretenda implementar, y observados con posterioridad sin que exista caducidad para los mismos.

Estos principios son:

- Principio de proactividad. Observación de la legalidad y la seguridad, con anterioridad a la implantación de la iniciativa, durante su vida útil y hasta el momento de su eliminación en la entidad, con adopción de las medidas previstas en la Ley.
- Principio de Privacidad por defecto. Adoptar la seguridad como un estándar en la concepción de cualquier actuación en la entidad que implique tratamiento de datos personales. Forma de trasmitir a los públicos con los que se relaciona la entidad, que la seguridad de su información personal es tratada con seguridad y confidencialidad.
- Principio de Privacidad desde el diseño. La Delegada de Protección de Datos debe estar presente en la concepción de cualquier iniciativa, de forma que se observe la legalidad y la seguridad desde la gestión de la iniciativa con el propósito de ahorrar tiempo y dinero en la entidad, y evitar tener que rehacer la iniciativa cuando ya está finalizada o implementada, por no cumplir con la legalidad vigente.

- Principio de Seguridad «end to end» (extremo a extremo, o de principio a fin). La seguridad debe estar garantizada en todas las etapas del proceso, así como en cambios sustanciales, sin exclusión ni excepción.

Estos procedimientos se acompañan de las siguientes características:

- La metodología de valoración de impacto debe ser sistemática y reproducible, con orientación a revisar procesos que den como resultado, la seguridad permanente del tratamiento de los datos personales.
- La funcionalidad, usabilidad y la configurabilidad de la iniciativa no es ajena al proceso y también debe ser atendida, en busca de un equilibrio satisfactorio.
- La disponibilidad de la iniciativa en múltiples plataformas no debe socavar los principios descritos ya que implica a la imagen y confiabilidad de la entidad respecto a los públicos con los que se relaciona.

5. Personal implicado.

De forma obligatoria, en la gestación de cualquier iniciativa que implique tratamiento de datos personales en Izenpe, deben participar los perfiles con capacidad de decisión, con la supervisión de la Delegada de Protección de Datos, como por ejemplo:

- Responsable del Departamento jurídico;
- Responsable de IT / Sistemas; y
- Responsable del/ de los departamento/s afectado/s

En última instancia, en la gestión del proyecto, se debe contemplar la descripción de los riesgos detectados, las medidas de seguridad implementadas para evitarlos, las medidas de seguimiento, los controles que se implantarán para asegurar que solo se tratan los datos personales necesarios y para las finalidades legítimas previstas y definidas. El resultado final debe ser un documento con un contenido mínimo y una estructura que deben definirse previamente.

6. Metodología.

La presente política establece la metodología para implantar un proceso para dar cumplimiento al mandato de garantizar la seguridad de los datos personales objeto de tratamiento y los derechos y deberes fundamentales de las personas establecido en el RGPD: «teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.» (art. 24.1 RGPD).

El Responsable de Seguridad y la Delegada de Protección de Datos velarán por que, en aplicación de la presente metodología, se garantice que en Izenpe no se implementarán procesos nuevos que:

- Traten datos personales que no sean necesarios para las finalidades del tratamiento (limitación de los datos tratados);

- En el nuevo proceso, no se tratarán los datos para finalidades diferentes a las previstas (limitación de la finalidad);
- En el análisis, se aplique la limitación del uso de los datos en el tiempo, de forma que no se traten más allá del tiempo necesario (limitación de tiempos de conservación); y
- Evitar el acceso a datos personales de personas que no precisen tratarlos (limitación de acceso).

La implementación de la presente política de privacidad por diseño y por defecto puede requerir la realización de una evaluación de impacto (que es objeto de un procedimiento específico) si se dan las condiciones de tratamiento de datos personales que pueda suponer riesgo para los derechos de las personas o para la seguridad de los datos personales.

7. Notificación de incidencias.

Cualquier incidencia significativa que se produzca en la implementación de esta política, o en cualquier fase de aplicación de la metodología propuesta, deberá ser comunicada al Responsable de Seguridad y/o a la Delegada de Protección de Datos, para que proceda a su valoración y actúe en consecuencia.

8. Consulta previa.

Si como consecuencia de la aplicación de esta política las conclusiones de cualquier análisis frente a un nuevo proceso, producto o servicio manifestaran un riesgo considerable para los datos personales o para los derechos de los interesados, se elevará consulta a la autoridad de control antes de proceder al tratamiento de los datos personales. Se obrará de esa forma cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.