Boletín 01/24

LOPD EN LA EMPRESA

EL RGPD UE 2016/679 EN APLICACIÓN

Transparencia de la información al interesado

El responsable del tratamiento de datos personales ha de llevar a cabo todas sus actividades aplicando el principio de transparencia en el tratamiento de los datos personales. Así viene regulado en la normativa aplicable a la protección de datos.

Esta transparencia se traduce en que el responsable cuando facilite la información a los interesados/as en todos sus aspectos debe realizarse:

- **De forma concisa**
- **Transparente**
- **Inteligible y de fácil acceso**
- **Con un lenguaje claro y sencillo en particular cualquier información dirigida específicamente a un menor.**

La información habrá que facilitarla por escrito o por otros medios, inclusive, a través de medios electrónicos. En el caso de que lo solicite el interesado, la información relativa al tratamiento de sus datos personales y/o ejercicio de derechos podrá facilitarse verbalmente siempre y cuando se demuestre la identidad del interesado que nos solicita la información por otros medios.

Contenido

IMPORTANTE

El incumplimiento del principio de transparencia supone una infracción regulada en la LOPDGDD

SANCIONES DE LA AEPD

Sancionada una Comunidad de propietarios por publicar datos personales de morosos en el tablón de anuncios

En la resolución de la AEPD https://www.aepd.es/documento/ps-00277-2023.pdf se sanciona a una Comunidad de bienes por la publicación de datos personales de morosos en un tablón de anuncios y por no aplicar las medidas de seguridad oportunas para evitar un acceso ilícito por parte de terceros a esos datos personales.

La parte reclamante manifestó en su escrito de reclamación que los datos de su número de apartamento y el importe de las deudas contraídas con la comunidad de vecinos se había expuesto en el tablón de anuncios, al que podía acceder cualquier persona que entrara en el edificio. Para ello se aportó como documentación relevante una fotografía del tablón de anuncios donde aparecen sus datos personales.

La AEPD sancionó a la Comunidad de bienes con una multa administrativa de 1.000€ por la vulneración de dos artículos de la normativa:

- **Infracción del artículo 5.1.f (RGPD)**; los datos se han de tratar garantizando una seguridad adecuada para evitar un tratamiento no autorizado garantizado la integridad y confidencialidad.
- **Infracción del artículo 32 (RGPD)**; el responsable del tratamiento no aplicó las medidas de seguridad adecuadas para garantizar la confidencialidad de los datos personales tratados por la Comunidad de propietarios.

Los principios relativos al tratamiento han de observarse con especial diligencia por los responsables y encargados del tratamiento.

IMPORTANTE

La AEPD en su escrito de reclamación ordena a la Comunidad de propietarios que retire el documento del tablón de anuncios y que disponga de un procedimiento para comunicar anuncios según la Ley de Propiedad Horizontal

LA AEPD ACLARA

Recomendaciones para usuarios en la utilización de *chatbots* con inteligencia artificial

Hoy en día, existe una proliferación de páginas web en las que podemos encontrar un *chatbot* que interactúa con el usuario. En la página de la AEPD hay publicada una infografía en la que se recogen unas recomendaciones básicas para tener en cuenta en relación con el sistema y el usuario:

Consejos generales en cuanto a los sistemas.

Revisar que se ofrece:

- Una política de privacidad y aviso legal que incluya una identificación clara y precisa del responsable del tratamiento
- Información sobre protección de datos con referencia al RGPD que incluya la información para poder ejercer los derechos.
- Información sobre si el *chatbot* continúa aprendiendo de las conversaciones mantenidas con los usuarios y que operaciones realiza con esos datos una vez mejorado.

Consejos para los usuarios.

No aceptar que:

- Se soliciten datos de registro que no sean necesarios.
- Se solicite el consentimiento sin definir para que van a ser tratados los datos y sin que permita retirarlo en cualquier momento.
- No facilitar datos personales de terceros si hay dudas de que el tratamiento va a trascender al ámbito doméstico.

IMPORTANTE

La AEPD alerta que dependiendo del tipo de sistema utilizado puede producir daño emocional, desinformación o inducir a engaño.

ACTUALIDAD LOPD

Resultados de la acción europea que ha analizado la designación y situación de los delegados de protección de datos

Fuente: AEPD

(18 de enero de 2024). La Agencia Española de Protección de Datos (AEPD) ha participado en una **acción europea coordinada** para analizar la designación y situación de los delegados de protección de datos (DPD) en entidades públicas y privadas, dentro del marco de actuaciones coordinadas del Comité Europeo de Protección de Datos (EDPB, por sus siglas en inglés). Este documento proporciona **una visión integral** para identificar y fomentar las mejores prácticas, detectar posibles deficiencias y realizar recomendaciones. La figura del delegado de protección de datos ejerce una función fundamental de intermediación entre las Autoridades de Supervisión, la ciudadanía y las organizaciones, y contribuye de manera esencial al cumplimiento de la normativa de protección de datos y a promover la protección efectiva de los derechos de los interesados. (…)

El informe recoge recomendaciones y puntos de atención dirigidos a las organizaciones, los DPD y las autoridades de control, tales como:

- Continuar promoviendo la concienciación entre las organizaciones para que adopten la necesaria diligencia en la designación del DPD.
- Necesidad de que los responsables del tratamiento verifiquen los medios puestos a disposición de los DPD para que desempeñen con eficacia las funciones que tienen encomendadas.
- Proporcionar la capacitación y la formación de los DPD a través de diversos mecanismos, así como fomentar el uso de la certificación.
- Necesidad de dotar al DPD de la debida independencia en el ejercicio de sus funciones con el fin de evitar los conflictos de interés, así como promover la necesaria visibilidad del delegado dentro de la organización.
- Importancia de promover los mecanismos internos para que el DPD reporte al más alto nivel de la organización. (…)

Puede ver más información en el siguiente enlace:

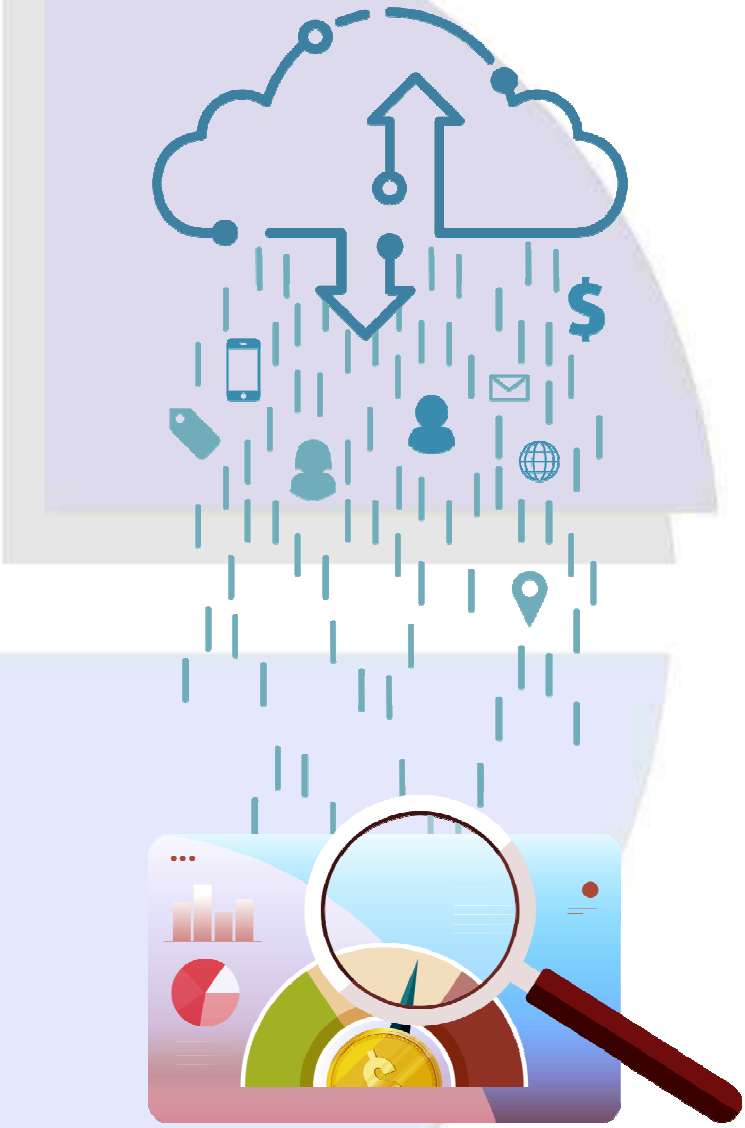
Appendix 1.2: National Reports on the CEF DPO (V.O)

EL PROFESIONAL RESPONDE

Nuevas tecnologías y ciberseguridad: amenazas y riesgos de las aplicaciones en la nube (II)

Las amenazas y riesgos que pueden ocurrir en este tipo de aplicaciones en la nube dependerán del servicio que contratemos.

Con carácter general podemos destacar las siguientes amenazas: accesos no autorizados; interfaces inseguras; uso de tecnologías compartidas; fuga de información; suplantación de identidad; falta de formación y desconocimiento del entorno; suplantación de identidad y ataques de *hacking*.



En la utilización de este tipo de aplicaciones, resulta imprescindible la realización de un análisis de riesgos y así poder aplicar las medidas necesarias para mitigar los riesgos. Los riesgos que pueden derivar de las amenazas indicadas anteriormente son, por ejemplo, acceso de usuarios con privilegios que actúan de forma maliciosa, desconocimiento de la localización de los datos, por ejemplo, cuando están ubicados en terceros países sin garantías adecuadas o falta de soporte en caso de que ocurra algún incidente y no se pueda acceder a los *logs* o registros de actividad. Una vez que conocemos los riesgos tendremos que aplicar las medidas de seguridad técnicas y organizativas más adecuadas para mitigarlos, por ejemplo, en el caso de falta de soporte, el proveedor debe garantizar que los *logs* y los datos se gestionen de una forma centralizada.

IMPORTANTE

En la contratación de aplicaciones en la nube es necesario que las medidas de seguridad técnicas y organizativas estén contenidas en el acuerdo de servicio

AUTOR: JULIO CÉSAR MIGUEL PÉREZ