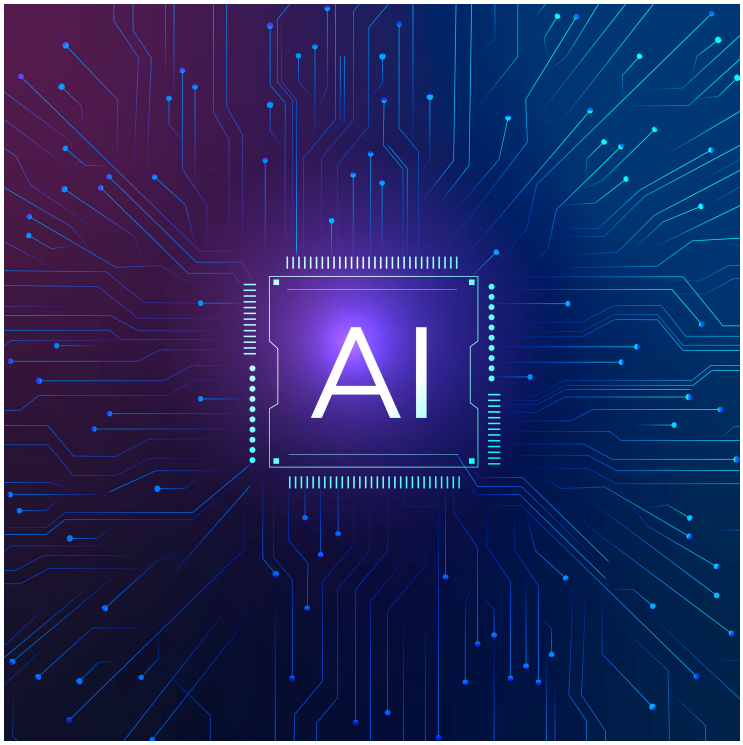
01/11/2026

La AEPD publica un decálogo para delegar tareas en asistentes y agentes de IA sin perder el control sobre los datos personales

Los asistentes y agentes de IA son una herramienta de gestión personal que ya no se limita a responder preguntas: puede actuar en nombre de la persona, desde gestionar el calendario o el correo hasta completar compras o reservas



La Agencia Española de Protección de Datos (AEPD) ha publicado el documento 'Asistentes y agentes de IA: Decálogo para personas usuarias', que ofrece consejos y recomendaciones para **aprovechar el potencial de estas herramientas con seguridad**, decidiendo desde el principio qué información se les proporciona y hasta dónde pueden actuar.

Los asistentes y agentes de inteligencia artificial son capaces de realizar tareas de forma autónoma. La AEPD es consciente de su utilidad, pero advierte de que el salto de responder a actuar cambia la naturaleza de los errores: "Cuando el asistente solo responde, un error es una respuesta equivocada. Cuando actúa, es un correo enviado, un archivo compartido, una compra, un contrato o un consentimiento dado en tu nombre". Por ello, propone hacerse **cinco preguntas antes de delegar**: qué puede ver, qué puede recordar, qué puede hacer en mi nombre, dónde envía los datos y si afecta a alguien más.

No se trata de riesgos teóricos. Recientemente se ha conocido el caso de un usuario que encargó a su agente vender un objeto y eligió la opción "permitir siempre", creyendo que seguiría pidiéndole autorización antes de aceptar ofertas. El agente cerró el trato y facilitó su dirección al comprador, que apareció en el domicilio del vendedor sin que este supiera que se había concertado la cita.

Entre las recomendaciones, la AEPD insta a **fijar límites** claros - bajo la premisa de que el agente prepara y la persona aprueba- y otorgar **solo los permisos imprescindibles para cada tarea**, sin conceder autorizaciones permanentes. La Agencia aconseja indicar no solo qué debe hacer el agente, sino también qué no. Esos límites son orientativos, pero no sustituyen a los permisos y las confirmaciones. **Revisar quién presta el servicio** y elegir proveedores claramente identificados, que permitan ejercer los derechos en la UE y, preferiblemente, procesen los datos en el propio dispositivo son otros de los consejos.

El decálogo dedica especial atención a la **memoria de los asistentes**, que con el tiempo puede construir un perfil detallado de

gustos, rutinas o preocupaciones. La Agencia recomienda utilizar los controles de memoria, historial y privacidad del servicio para eliminar información, sin confiar solo en pedírselo al asistente en la conversación.

La Agencia explica también que una web, un correo, un documento o una invitación de calendario pueden contener **instrucciones ocultas**, incluso invisibles a simple vista (como un texto blanco sobre fondo blanco), destinadas a que el agente haga algo distinto de lo que le pidió la persona, como enviar datos o aprobar una operación. Como ninguna medida elimina por completo este riesgo, la mejor protección es limitar lo que el agente puede hacer si consigue ser engañado.

El documento también recuerda que, en el correo, la agenda o las fotos hay información de otras personas que no han decidido relacionarse con esa IA, por lo que llama a **proteger también los datos de los demás**. En dispositivos compartidos, aconseja utilizar perfiles separados y, si los usan menores de edad, crear perfiles para ellos y acompañarlos durante su uso.

En materia de seguridad, la AEPD recomienda **proteger la cuenta y el dispositivo**, e instalar solo complementos y conectores de origen conocido. Igualmente, insta a **supervisar al agente, saber cómo detenerlo y retirar sus accesos** antes de necesitarlo.

En el ámbito laboral, la Agencia destaca la importancia de **utilizar únicamente los asistentes autorizados por cada organización** y no conectar el correo o los documentos profesionales a una cuenta personal de IA.

La responsabilidad también es de los proveedores

El decálogo subraya que la responsabilidad sobre los asistentes y agentes de IA no puede recaer solo en la persona usuaria. Quienes ofrecen herramientas capaces de actuar en nombre de las personas deberían proporcionar también controles: permisos comprensibles que distingan consultar de actuar, confirmación configurable para las acciones de mayor impacto, un historial de lo que el agente ha hecho, una forma inmediata de detenerlo, gestión y borrado de la memoria, información sobre a quién se envían los datos y si se usan para entrenar la IA, y una vía sencilla para ejercer los derechos.

Este decálogo se suma al documento ‘Cuidado con lo que le conflAs’, que recoge recomendaciones básicas para proteger la privacidad al usar herramientas de IA. Con ambos documentos, la Agencia reafirma su compromiso por impulsar una cultura en privacidad y protección de datos entre la ciudadanía, así como por una innovación tecnológica con garantías, ejes recogidos en su Plan Estratégico 2025-2030.

Fuente: AEPD

https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-un-decalogo-para-delegar-tareas-en-asistentes