Bonn, Bucarest, Dublín, Lisboa, Madrid, Milán, París, La Haya, Viena, Varsovia

¿Es el DPO la persona adecuada para ser el Responsable de IA?

Serie de microinformes del Grupo de Trabajo sobre IA y Datos de CEDPO
Julio de 2024

Autores:
Marc Bellon
Lionel Capel
Ernst-Oliver Wilhelm
Maria Moloney

Información de contacto:
https://cedpo.eu
info@cedpo.eu

Acerca de la serie Micro-Insights

La serie Micro-Insights es una iniciativa editorial del Grupo de Trabajo sobre IA y Datos de CEDPO. Ofrecerá artículos breves, digeribles y definitivos sobre áreas clave de interés en la intersección entre los datos y la inteligencia artificial. Con un enfoque práctico, centrado por un lado en la explicación de temas complejos y por otro en su aplicación, se destacará la importancia de las áreas clave y se asesorará a los profesionales sobre el impacto y los próximos pasos. Con la entrada en vigor de la Ley de Inteligencia Artificial de la UE (la "AI Act") en 2024, el escenario está ahora preparado para todos los profesionales, y es posible debatir la regulación de los datos y la IA con mucha más claridad.

La serie Micro-Insights seguirá la evolución de la IA y los datos en los próximos años y, a medida que se acerque el final del periodo crucial de aplicación de la AI Act y que las tecnologías de IA evolucionen de forma cada vez más novedosa e inesperada, la serie responderá con orientaciones actualizadas y autorizadas sobre los principales ámbitos de interés.

Entre otros temas, analizaremos:

- Regulación de los Sistemas de Inteligencia Artificial de Propósito General según la AI Act.
- Comentarios al Pacto de IA.
- Formación para profesionales de protección de datos sobre la realización de evaluaciones de impacto sobre derechos fundamentales según la AI Act.
- El papel que tendrán los reguladores de protección de datos en la regulación de la IA.
- Examinar si el Delegado de Protección de Datos es o no es la persona adecuada para ser el "IA Officer"
- La base legal para el uso de datos de entrenamiento en el aprendizaje automático.
- El conjunto de herramientas de preparación para la AI Act.

Índice

1. La evolución del papel de responsable de protección de datos

La función del delegado de protección de datos (DPO) en Europa los últimos seis años, desde la llegada del Reglamento general de protección de datos (RGPD), ha evolucionado y se ha ampliado en consonancia con el creciente uso de la tecnología y los datos en las organizaciones. El tratamiento tanto de datos como de datos personales ha crecido exponencialmente en la Unión Europea (UE) y también a nivel mundial. Como consecuencia, muchos países están empezando a seguir los pasos de la UE introduciendo sus propias versiones de normativa sobre protección de datos.

Aunque el RGPD tiene seis años, incluye disposiciones sobre la toma de decisiones automatizadas. Ahora, en la era de la Inteligencia Artificial (IA), estas disposiciones facultan a los DPO para regular el uso de la IA en el tratamiento de datos personales. El RGPD concede a los interesados el derecho a oponerse a la toma de decisiones automatizadas, especialmente las decisiones basadas únicamente en la elaboración de perfiles, si tales decisiones tienen consecuencias jurídicas o personales significativas. Por lo tanto, los DPO deben garantizar que los interesados tengan la posibilidad de solicitar la intervención humana o alguna otra forma de impugnar las decisiones automatizadas. Además, el DPO también tiene la responsabilidad de realizar comprobaciones rutinarias para asegurarse de que los sistemas automatizados funcionan según lo previsto.

Con arreglo a la AI Act de la UE, muchos tipos de sistemas automatizados de toma de decisiones entran en la categoría de sistemas de alto riesgo. Cuando tales sistemas procesan datos personales, los DPO deben garantizar que se llevan a cabo evaluaciones de impacto sobre la protección de datos (EIPD) y que se introducen las salvaguardias adecuadas cuando sea necesario antes de proceder a la implantación de tales sistemas.

El 7 de diciembre de 2023, el Tribunal de Justicia de la Unión Europea (TJUE) dictó una sentencia histórica contra la agencia alemana de calificación crediticia Schufa AG Holding ("SHUFA"), que reforzó los derechos individuales en torno a la calificación crediticia automatizada. El Tribunal sostuvo que la creación de una calificación crediticia constituía una "decisión individual automatizada" de conformidad con el artículo 22 del RGPD de la UE. Esta decisión fue significativa porque concedió a los interesados el derecho a oponerse a dichas calificaciones y a solicitar la intervención humana en el proceso de creación. Aunque la calificación crediticia sigue estando permitida, el TJUE subrayó la necesidad de establecer medidas para salvaguardar la equidad y los derechos individuales.

Desde una perspectiva más general, la sentencia del TJCE puede afectar a los proveedores de servicios que emplean procesos automatizados para generar puntuaciones basadas en el riesgo u otros resultados, especialmente si dichos resultados desempeñan un papel fundamental en las decisiones que afectan significativamente a los interesados. Sobre la base de esta evaluación, la sentencia refuerza claramente la posición del DPO en torno a sus obligaciones de proteger los datos personales utilizados en cualquier tipo de proceso automatizado de toma de decisiones. Tal vez de ahí haya surgido la idea de que el DPO asuma el papel de responsable

de la IA en las organizaciones. Esta idea, sin embargo, es más compleja tras una reflexión y se analiza a continuación.

2. Es el DPO el mejor posicionado para convertirse en responsable de la IA

Independientemente de si los DPO asumen la plena responsabilidad del cumplimiento de la IA en una organización, es evidente que deben formar parte del debate siempre que los sistemas de IA procesen datos personales. Además, en la actualidad no existe una interpretación universalmente aceptada del término "responsable de la IA" y, a diferencia del DPO, cuya designación y responsabilidades se definen en los artículos 37 a 39 del RGPD, la AI Act no define la función de un responsable de la IA, ni exige específicamente el nombramiento de un responsable de la IA.

El nombramiento de un responsable de IA o quizás de un *director* de IA es un paso probable para algunas organizaciones en un futuro próximo. Con la inclusión de la gestión de riesgos y el cumplimiento en esta función, y dependiendo de la naturaleza de las especificaciones del puesto, podría haber limitaciones potenciales a la eficacia del responsable de IA. Un responsable de IA centrado únicamente en el riesgo y el cumplimiento podría perderse el potencial de la IA para la transformación, el aumento de la eficiencia y las nuevas oportunidades de negocio. Por tanto, ascender al DPO a esta función podría plantear retos, como se expone a continuación.

- Asignar a un DPO poderes de decisión sobre la gobernanza de la IA puede crear un conflicto de intereses con arreglo al artículo 38 del RGPD. Este artículo prohíbe las situaciones en las que la misma persona es responsable tanto de la ejecución de las actividades de tratamiento de datos como de garantizar el cumplimiento de las normas de protección de datos.
- Además, asignar la función de responsable de la IA al DPO podría comprometer su independencia, un aspecto crucial del cargo de DPO según lo dispuesto en el RGPD. Es probable que las organizaciones necesiten líneas claras de autoridad y funciones diferenciadas para la aplicación de la IA y la supervisión de la protección de datos.

Como alternativa, algunas organizaciones podrían crear una función de "responsable de riesgos de IA". Esta función podría centrarse en la gestión de riesgos y el cumplimiento, garantizando que los sistemas de IA (IAS) se adhieran al enfoque basado en el riesgo descrito en la AI Act. El responsable de riesgos de la IA también podría tener en cuenta los principios éticos para promover una IA digna de confianza. Aunque esta función se solapa en cierta medida con las responsabilidades del DPO, especialmente en los aspectos de protección de datos, no abarcaría todo el alcance de una función de responsable de IA centrada en impulsar la transformación y la oportunidad de la IA.

Consideremos los tres escenarios siguientes:

2.1 Responsable de IA en pequeñas y medianas empresas

Debido a la falta de recursos y/o empleados con las competencias necesarias, los DPO se convierten en responsables tanto de la protección de datos como del cumplimiento de la IA. En este caso, es poco probable que un DPO pueda supervisar una gran función de protección de datos y de cumplimiento de la IA en paralelo. Los casos probables de uso de la IA en tales organizaciones serían la gobernanza de chatbots y herramientas como ChatGPT o Copilot, así como la supervisión del SIA de algunos proveedores. Un DPO de este tipo necesitaría, por tanto, desarrollar sus habilidades en la gobernanza generativa de la IA para poder asumir estas nuevas responsabilidades.

2.2 Responsable de IA en grandes organizaciones

La implantación paralela de la protección de datos y el cumplimiento de la IA parece más probable en las grandes organizaciones. Estos casos de uso podrían incluir:

- el uso de la IA en paquetes de software o soluciones empresariales.
- crear sistemas internos de IA con o sin el apoyo de socios externos. Sin embargo, el desarrollo y despliegue de tales sistemas daría lugar a que la organización fuera clasificada como desarrolladora o desplegadora de sistemas de IA con arreglo a la AI Act de la UE. Esto obligaría a la empresa a cumplir todas las consecuencias normativas que ello conlleva.

Aunque el cumplimiento de la normativa sobre IA podría no ser competencia directa del DPO, su experiencia sería crucial en áreas que se solapan significativamente con los requisitos del RGPD. Esto incluiría la protección de datos, la detección de sesgos (especialmente en sistemas de IA de alto riesgo) y la evaluación de la supervisión humana obligatoria tanto para las operaciones del sistema como para las consideraciones de derechos fundamentales.

2.3 Responsable de IA en organizaciones de desarrollo y despliegue de IA

La Ley de Inteligencia Artificial de la UE impone funciones distintas a los desarrolladores y a los implantadores de sistemas de IA. Ambas entidades tienen responsabilidades distintas en virtud de la Ley para garantizar el uso seguro y responsable de la IA. Los DPO de estas organizaciones necesitarán conocimientos específicos y especializados de sus sistemas internos de IA si quieren comprender plenamente y mantenerse al corriente de las funciones de estos sistemas tan propensos al cambio y la adaptación (aprendizaje) ante nuevos requisitos e implantaciones.

3. Conclusión

En resumen, los delegados de protección de datos podrían asumir la función de responsable de la IA (AI Officer) en determinadas situaciones, ya que existe un solapamiento significativo en los aspectos éticos, jurídicos y de gobernanza de estas dos funciones. Sin embargo, definir claramente el alcance, las obligaciones y las expectativas de la función de responsable de la

IA puede ayudar a determinar si el DPO podría hacer una transición efectiva a este nuevo puesto o incluso incorporarlo a su función actual de protección de datos.

Independientemente del tamaño o el escenario de la organización, los responsables de la protección de datos deben contar con mayores responsabilidades, como mínimo para garantizar que los sistemas de IA cumplen los requisitos de protección de datos.

Desde una perspectiva más general, la posible fusión de las funciones de DPO y IA Officer podría estar señalando un cambio significativo que está teniendo lugar en el campo de la gobernanza, el riesgo y el cumplimiento (GRC). Este cambio podría requerir la creación de un nuevo puesto de liderazgo, posiblemente algo parecido al de Director de Cumplimiento de Datos, que supervisaría el cumplimiento de todos los datos y proyectos digitales y sistemas organizativos.