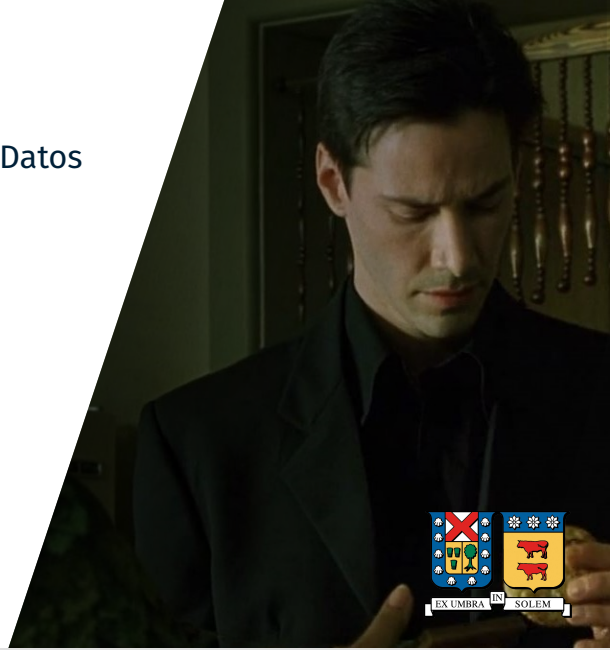
GDPR

Reglamento General de Protección de Datos



Informática Legal y Derecho Informático
INF300 - 2025-2

Toledo Correa, Pedro

Departamento de Informática
Universidad Técnica Federico Santa María

29 de octubre de 2025 - v1.0

Tabla de contenidos

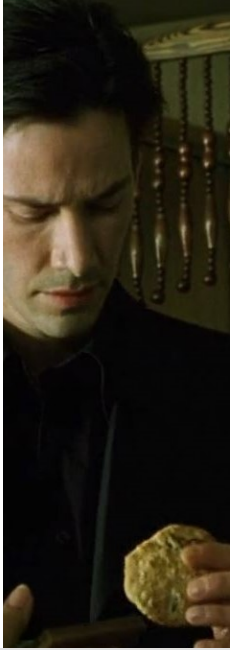
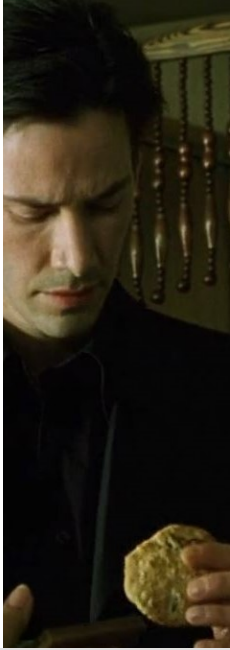
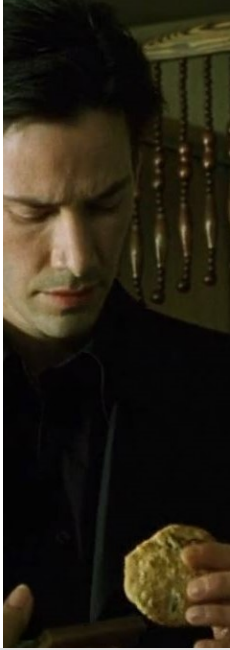


Tabla de contenidos



Origen y Motivación del GDPR

- Adoptado por la UE en 2016, en vigencia desde mayo de 2018
- Responde a la creciente digitalización y globalización
- Basado en la Directiva 95/46/CE[1]
- Establece protección de datos como derecho fundamental de la UE[2]

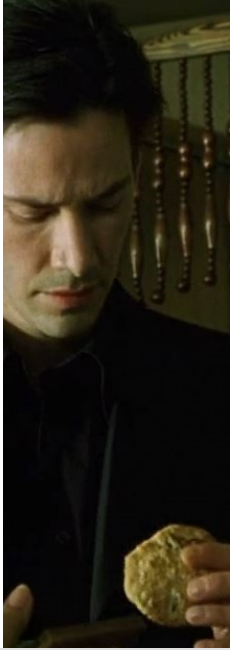


[1] https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A31995L0046

[2] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12016P%2FTXT

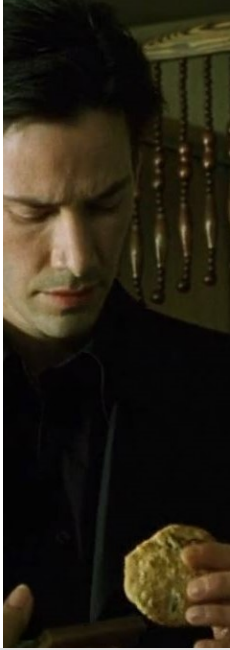
Evolución de la Normativa de Privacidad en Europa

- Directiva 95/46/CE estableció las bases
- Necesidad de una normativa actualizada ante el avance tecnológico
- GDPR unifica y fortalece derechos de privacidad a nivel europeo



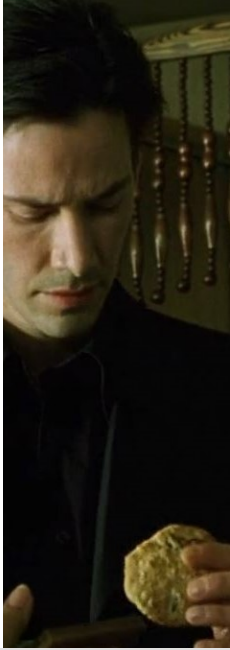
Objetivos Principales del GDPR

- Protección de datos personales[3]
- Derechos de los individuos sobre sus datos personales
- Responsabilidad de empresas y gobiernos en el tratamiento de datos



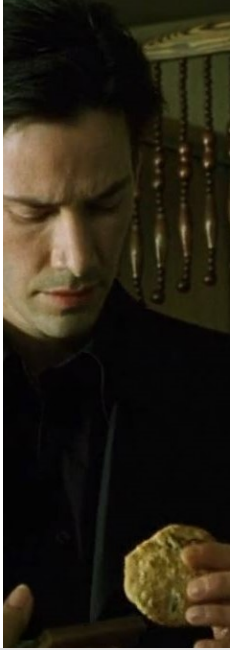
[3] https://gdpr-info.eu/art-1-gdpr/

Tabla de contenidos



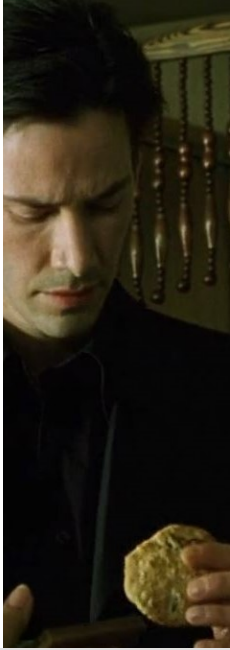
Definiciones - Artículo 4

- Datos personales
- Tratamiento
- Limitación del tratamiento
- Creación de perfiles
- Seudonimización
- Fichero
- Responsable del tratamiento
- Encargado del tratamiento
- Destinatario



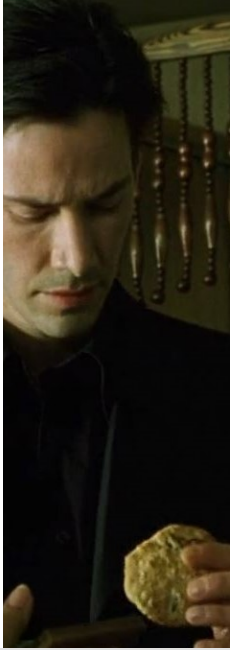
Definiciones - Artículo 4

- Tercero
- Consentimiento del interesado
- Violación de la seguridad de los datos personales
- Datos genéticos
- Datos biométricos
- Datos relativos a la salud
- Establecimiento principal
- Representante
- Empresa



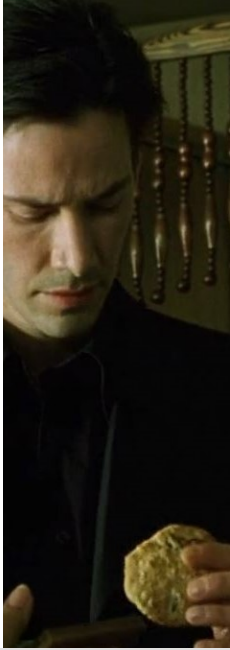
Definiciones - Artículo 4

- Grupo empresarial
- Normas corporativas vinculantes
- Autoridad de control
- Autoridad de control interesada
- Tratamiento transfronterizo
- Información relevante y fundamentada
- Servicio de información de la sociedad
- Organizaciones internacionales



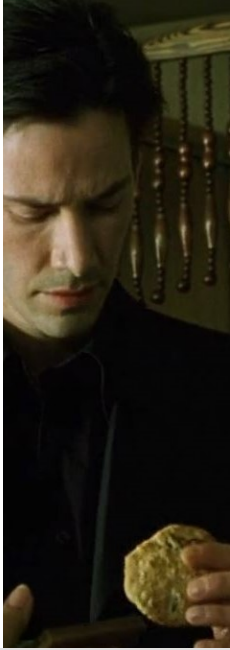
Artículo 4.1 - Datos Personales

- Cualquier información que permita identificar a una persona física, ya sea directamente o de forma indirecta
- Esta definición incluye una amplia gama de datos, desde nombres hasta identificadores online
- Se considera “identificable” a la persona cuando puede ser identificada, directa o indirectamente, con la ayuda de información adicional
- Los datos personales deben ser tratados con especial atención para garantizar su privacidad y protección
- Ejemplo: Nombre, dirección de correo electrónico, número de teléfono, datos de ubicación



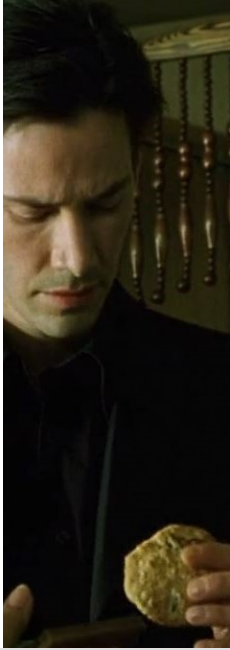
Artículo 4.2 - Tratamiento

- El “tratamiento” cubre cualquier operación realizada sobre los datos personales, ya sea de forma automatizada o no
- Incluye acciones como la recolección, grabación, organización, estructuración, conservación, modificación, recuperación, consulta, difusión, etc.
- Abarca todo tipo de procesamiento de datos, incluso la eliminación o destrucción de los mismos
- El tratamiento debe cumplir con los principios establecidos en el GDPR para garantizar la protección de los datos personales
- Ejemplo: Recolectar información de contacto de un usuario para fines de marketing



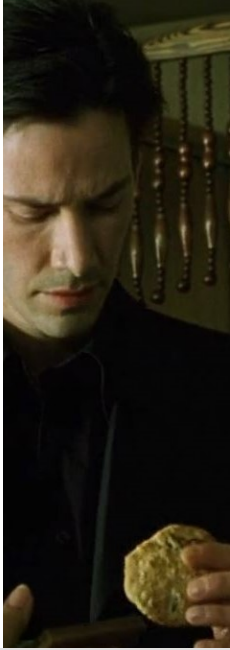
Artículo 4.3 - Limitación del Tratamiento

- Los datos deben ser tratados de acuerdo con la finalidad para la cual fueron recolectados
- El tratamiento de datos debe estar restringido a lo estrictamente necesario para cumplir con dichos fines
- Es fundamental no usar los datos para propósitos distintos a aquellos que fueron explícitamente informados al usuario
- Esta limitación ayuda a evitar la recopilación de datos excesivos y asegura que los datos no sean mal utilizados
- Ejemplo: Los datos de contacto recolectados para un evento no deben ser utilizados para campañas publicitarias sin el consentimiento explícito



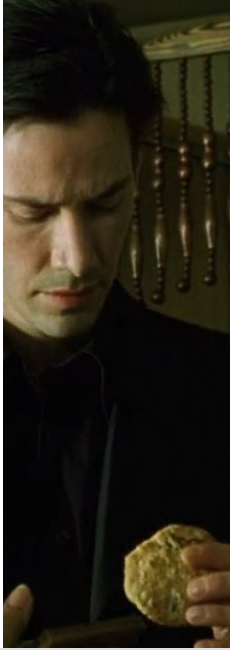
Artículo 4.4 - Profiling (Elaboración de Perfiles)

- El “profiling” se refiere a cualquier tipo de tratamiento automatizado de datos personales para evaluar aspectos personales, como rendimiento, salud, preferencias, etc.
- El profiling puede ser utilizado para predecir comportamientos futuros o tomar decisiones automatizadas sobre una persona
- A menudo, el profiling se realiza a través de algoritmos y técnicas automatizadas, sin intervención humana directa
- Es necesario garantizar que el interesado sea informado sobre el uso de sus datos para profiling y se les ofrezca la posibilidad de oponerse a ello
- Ejemplo: Un sistema que utiliza los datos de compra para predecir qué productos podría comprar un cliente en el futuro



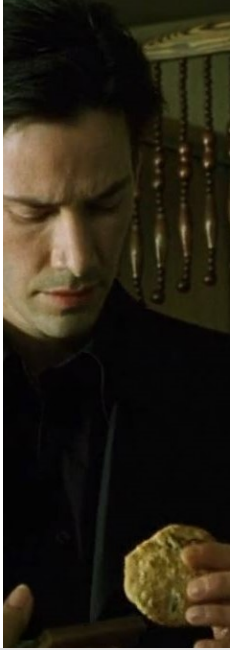
Artículo 4.7 - Encargado del Tratamiento

- El encargado del tratamiento es la persona o entidad que procesa los datos personales en nombre del responsable del tratamiento
- El encargado debe cumplir con las instrucciones del responsable y garantizar que se implementen las medidas de seguridad adecuadas
- El responsable del tratamiento sigue siendo el titular de la responsabilidad sobre el uso de los datos, mientras que el encargado gestiona el procesamiento
- Los acuerdos entre el responsable y el encargado deben formalizarse en un contrato que detalle los términos y condiciones del tratamiento
- Ejemplo: Un proveedor de servicios en la nube que procesa los datos personales de los usuarios en nombre de una empresa



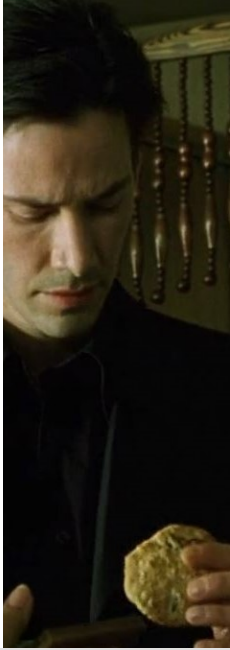
Artículo 4.10 - Tercera Parte

- Se entiende por tercera parte a cualquier persona u organización distinta del interesado, del responsable o del encargado del tratamiento, que recibe los datos personales
- Las terceras partes pueden tener acceso a los datos si el responsable lo autoriza, siempre que se sigan los principios de protección de datos
- Las terceras partes pueden incluir socios comerciales, proveedores de servicios o incluso entidades gubernamentales
- Es esencial garantizar que las terceras partes que reciban los datos personales también respeten la normativa de protección de datos
- Ejemplo: Un socio comercial que recibe datos personales para proporcionar servicios adicionales como soporte técnico



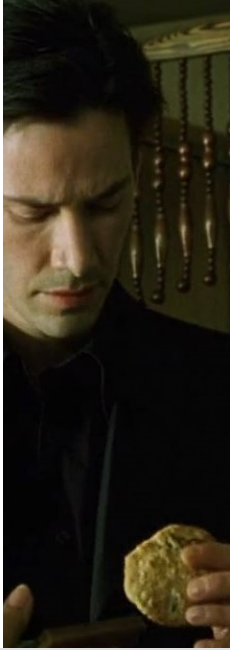
Artículo 4.11 - Consentimiento

- El consentimiento es una manifestación libre, específica, informada e inequívoca de la voluntad del interesado para aceptar el tratamiento de sus datos personales
- El consentimiento debe ser dado mediante una acción clara, como marcar una casilla o firmar un formulario
- El interesado tiene el derecho a retirar su consentimiento en cualquier momento, lo cual debe ser tan fácil como darlo
- El responsable debe ser capaz de demostrar que se ha obtenido el consentimiento del interesado de manera adecuada
- Ejemplo: Marcar una casilla para consentir recibir comunicaciones de marketing por correo electrónico



Artículo 4.18 - Empresa

- Una “empresa” se refiere a cualquier entidad, ya sea pública o privada, que trate datos personales dentro de sus actividades económicas
- El término “empresa” abarca a organizaciones de cualquier tamaño, desde pequeñas empresas hasta grandes corporaciones multinacionales
- La empresa debe asegurarse de cumplir con los principios y obligaciones establecidos en el GDPR al manejar los datos personales de sus clientes y empleados
- Las empresas tienen la responsabilidad de garantizar que los datos personales sean tratados de manera legal, justa y transparente
- Ejemplo: Una empresa de telecomunicaciones que procesa datos personales de sus clientes para ofrecerles servicios



Artículo 4.24 - Objeción Razonada y Relevante

- La objeción razonada y relevante es el derecho del interesado a oponerse a decisiones basadas únicamente en el tratamiento automatizado de sus datos, como la elaboración de perfiles
- El interesado tiene el derecho de impugnar decisiones que le afecten significativamente, como ser incluido en una lista de clientes potenciales basándose en su comportamiento de compra
- Si el interesado presenta una objeción, el responsable del tratamiento debe realizar una evaluación para determinar si se mantiene la decisión automatizada o si se requiere una intervención humana
- Es importante que el interesado sea informado de su derecho a oponerse y se le brinden los medios para ejercerlo
- Ejemplo: Un cliente que se opone a recibir ofertas personalizadas basadas en su comportamiento en línea

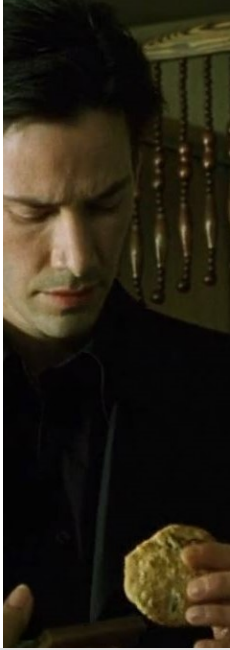
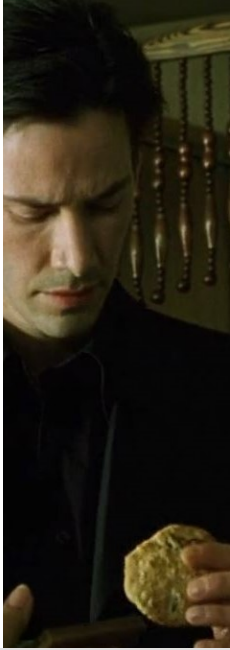
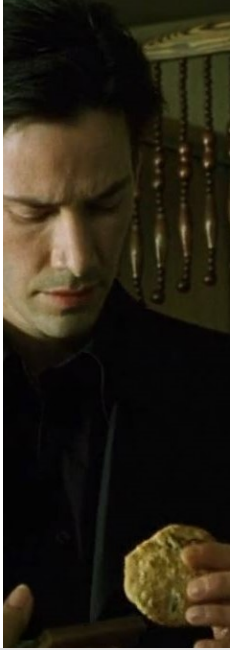


Tabla de contenidos



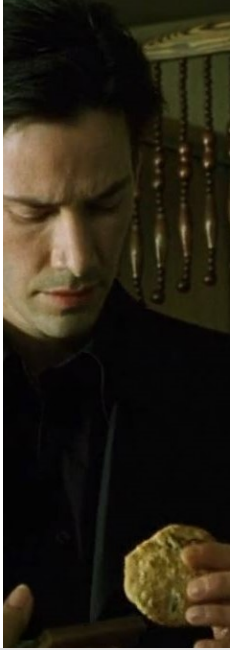
Artículo 5.1.a - Licitud, Lealtad y Transparencia

- Los datos deben ser tratados de manera lícita, leal y transparente para el interesado
- El tratamiento de datos debe basarse en principios fundamentales, asegurando que los derechos de los individuos sean respetados
- La información proporcionada al usuario debe ser clara, concisa, fácilmente accesible y comprensible, usando un lenguaje claro y sencillo
- Los responsables del tratamiento deben informar a los interesados sobre la base legal que justifica el tratamiento de sus datos, incluyendo los fines específicos de la recolección y el uso de estos datos
- Ejemplo: Cuando un usuario se registra en un servicio online, la empresa debe explicar de manera clara para qué usará los datos y si se compartirán con terceros



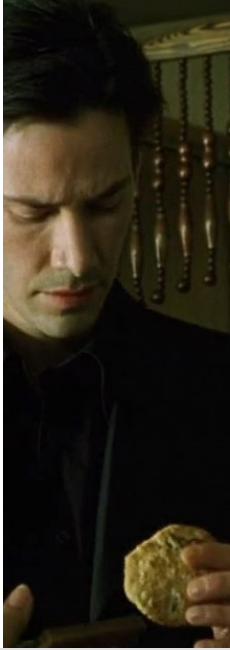
Artículo 5.1.b - Limitación de la Finalidad

- Los datos personales deben ser recolectados con fines específicos, explícitos y legítimos
- No se deben utilizar para fines incompatibles con aquellos para los cuales fueron recolectados inicialmente
- Las organizaciones deben asegurarse de que la recolección de datos sea adecuada y relevante para los fines establecidos, sin que se extralimiten
- Ejemplo: Si una empresa recopila datos de un cliente para ofrecerle un servicio, no puede usar esos mismos datos para fines de marketing sin el consentimiento explícito del cliente



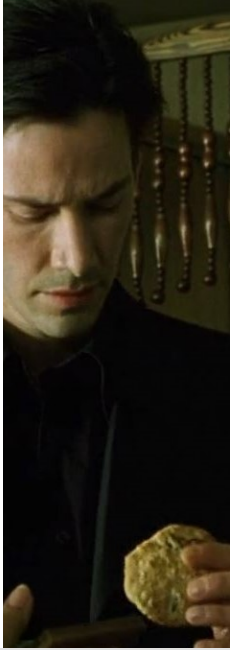
Artículo 5.1.c - Minimización de Datos

- Solo se deben recolectar los datos que sean estrictamente necesarios para cumplir con los fines del tratamiento
- El principio de minimización establece que se deben evitar la recolección de datos excesivos o irrelevantes en relación con los objetivos específicos del tratamiento
- Este principio también se extiende a la cantidad de datos almacenados, limitando solo a lo necesario para el propósito específico
- Ejemplo: Si una tienda online solicita información de contacto para procesar un pedido, no debe pedir datos adicionales como la fecha de nacimiento o la ocupación del cliente si no son relevantes para el proceso



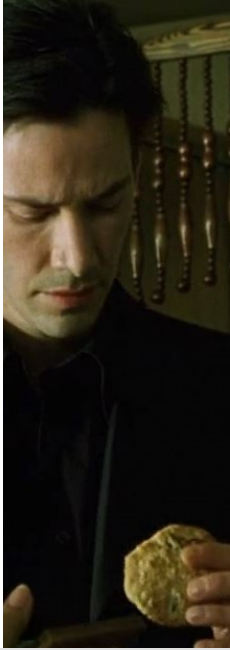
Artículo 5.1.d - Exactitud

- Los datos personales deben ser exactos y, cuando sea necesario, actualizados
- Se deben tomar todas las medidas razonables para asegurar que los datos personales sean correctos, especialmente si se usan para la toma de decisiones importantes para los interesados
- Las organizaciones deben contar con procedimientos que permitan rectificar los datos inexactos o incompletos en un plazo razonable
- Ejemplo: Si una dirección de correo electrónico registrada se vuelve incorrecta, debe ser corregida de inmediato



Artículo 5.1.e - Limitación del Plazo de Conservación

- Los datos personales solo deben almacenarse durante el tiempo necesario para los fines para los cuales fueron recolectados
- Una vez que los datos ya no sean necesarios, deben ser eliminados o anonimizados para garantizar que no se sigan procesando
- Las organizaciones deben establecer políticas claras de conservación de datos y asegurarse de que no se conserven más tiempo del necesario
- Ejemplo: Una tienda online debe eliminar los datos de un cliente que no ha realizado compras en más de un año, a menos que haya una obligación legal de conservarlos durante más tiempo



Artículo 5.1.f - Integridad y Confidencialidad

- Los datos personales deben ser procesados de manera que garantice su seguridad, incluyendo protección contra accesos no autorizados o ilícitos y contra la pérdida, destrucción o daño accidental
- Las organizaciones deben implementar medidas técnicas y organizativas adecuadas, como firewalls, protocolos de encriptación, y acceso restringido a los datos
- Además, deben asegurarse de que los empleados y terceros con acceso a los datos sean capacitados y conscientes de las políticas de seguridad y privacidad
- Ejemplo: El uso de encriptación para proteger la información personal de los usuarios en bases de datos y durante la transmisión de datos por internet

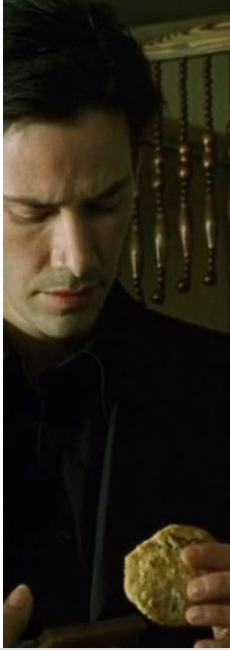
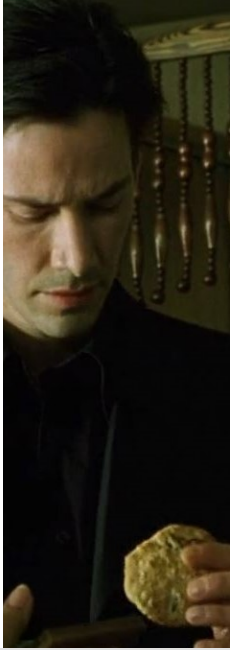
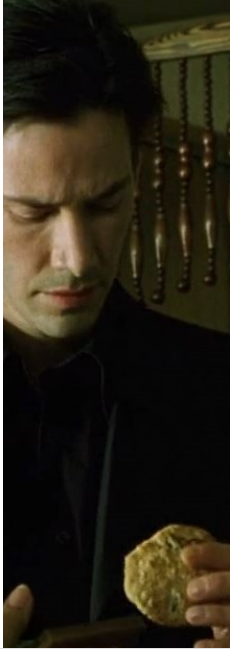


Tabla de contenidos



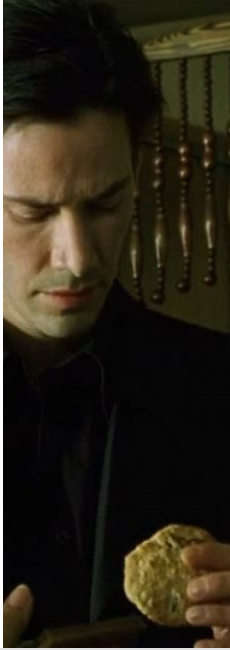
Artículo 15 - Derecho de Acceso

- Regula el derecho del interesado a obtener confirmación sobre el tratamiento de sus datos personales y a acceder a los mismos
- El interesado tiene derecho a conocer si sus datos están siendo tratados y recibir información detallada sobre ese tratamiento



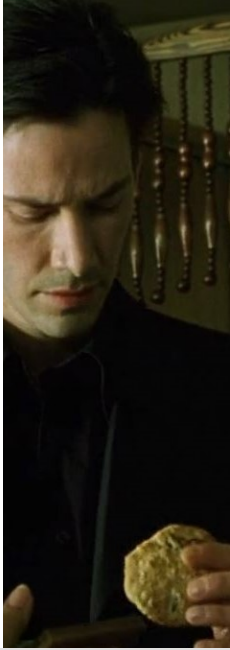
Artículo 16 - Derecho de Rectificación

- Establece el derecho del interesado a rectificar datos personales inexactos o incompletos que le conciernan
- El interesado puede solicitar que se corrijan o completen los datos que están siendo tratados



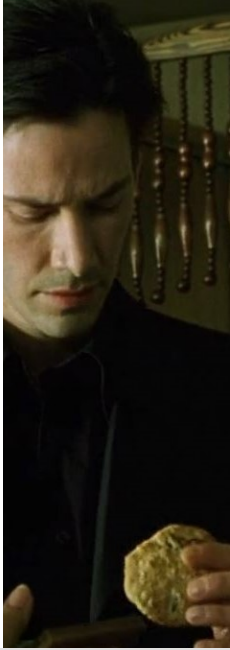
Artículo 17 - Derecho al Olvido

- Regula el derecho a la supresión de los datos personales cuando ya no sean necesarios para los fines para los que fueron recabados
- El interesado puede solicitar la eliminación de sus datos, por ejemplo, cuando estos ya no sean necesarios o tras la finalización de un contrato



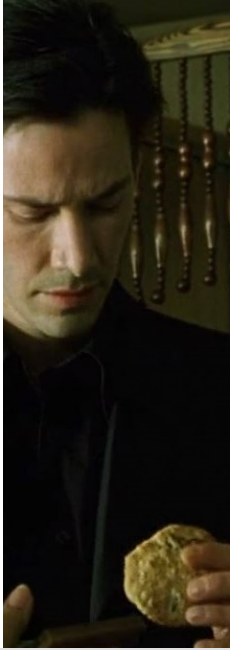
Artículo 18 - Derecho a la Limitación del Tratamiento

- Establece el derecho a limitar el tratamiento de los datos cuando se cuestione su exactitud o cuando el tratamiento sea ilegal
- El interesado puede solicitar que se restrinja el uso de sus datos mientras se resuelven las disputas sobre su exactitud



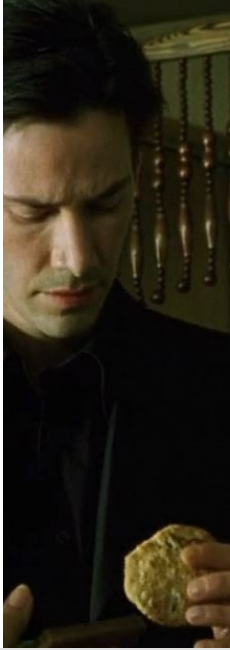
Artículo 19 - Obligación de Notificación

- Impone la obligación de notificar al interesado y a las autoridades de control cualquier rectificación, eliminación o limitación del tratamiento
- La notificación incluye la rectificación, eliminación o restricción del tratamiento de datos personales por parte de terceros



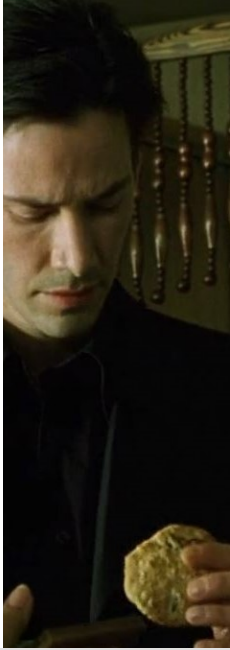
Artículo 20 - Derecho a la Portabilidad de los Datos

- Regula el derecho del interesado a recibir sus datos personales en un formato estructurado y de uso común, y a transferirlos a otro responsable
- El interesado puede solicitar la transferencia de sus datos a otro responsable sin obstaculizar el tratamiento



Artículo 21 - Derecho de Oposición

- Establece el derecho del interesado a oponerse al tratamiento de sus datos personales en función de intereses legítimos
- El interesado puede oponerse al tratamiento cuando considere que sus derechos y libertades prevalecen sobre los intereses del responsable



Artículo 22 - Decisiones automatizadas

- Regula la toma de decisiones automatizadas, incluida la elaboración de perfiles, que tenga efectos jurídicos sobre el interesado
- La protección contra decisiones automatizadas tiene como objetivo garantizar la no discriminación y el respeto de los derechos fundamentales

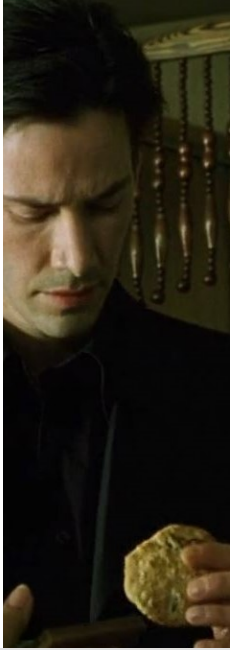
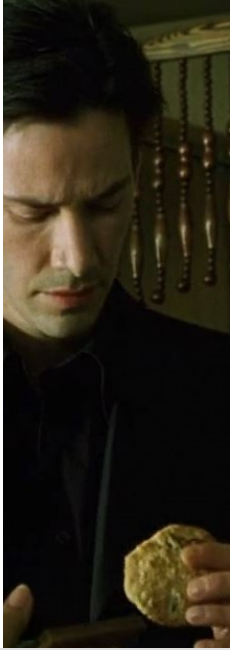
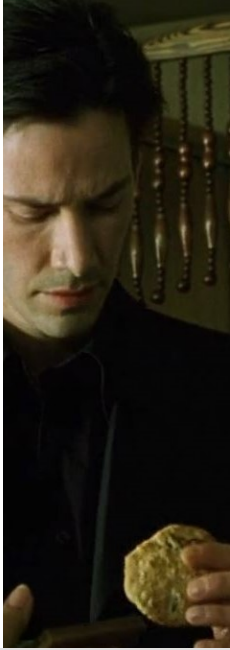


Tabla de contenidos



Artículo 35 - Evaluación de Impacto (DPIA)

- La Evaluación de Impacto sobre la Protección de Datos (DPIA) es un proceso para identificar y mitigar los riesgos asociados al tratamiento de datos personales
- Se debe realizar una DPIA cuando el tratamiento de datos pueda afectar de manera significativa los derechos y libertades de las personas, especialmente cuando se utilizan nuevas tecnologías
- La DPIA debe incluir:
  - Descripción del tratamiento y sus fines
  - Evaluación de la necesidad y proporcionalidad del tratamiento
  - Evaluación de los riesgos para los derechos y libertades de los interesados
  - Medidas adoptadas para mitigar esos riesgos
- Si, después de realizar la DPIA, persisten riesgos elevados, el responsable del tratamiento debe consultar a la autoridad de protección de datos antes de proceder con el tratamiento



Artículo 37 - Delegado de Protección de Datos (DPO)

- El Delegado de Protección de Datos (DPO) debe ser designado por ciertas entidades que procesen datos de manera habitual y a gran escala
- El DPO tiene como responsabilidad supervisar el cumplimiento del GDPR dentro de la organización, proporcionar asesoramiento y actuar como punto de contacto con las autoridades de protección de datos
- La designación del DPO es obligatoria para:
  - Autoridades o organismos públicos
  - Entidades cuyo tratamiento implique una vigilancia regular y sistemática de interesados a gran escala
  - Entidades cuyo tratamiento de datos sea a gran escala y esté relacionado con categorías especiales de datos (por ejemplo, datos de salud)
- El DPO debe ser independiente, experto en protección de datos, y tener la autoridad necesaria para realizar sus tareas sin interferencias externas

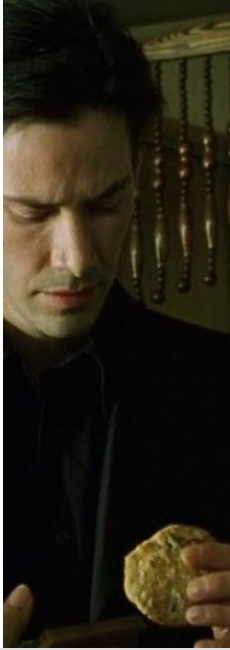
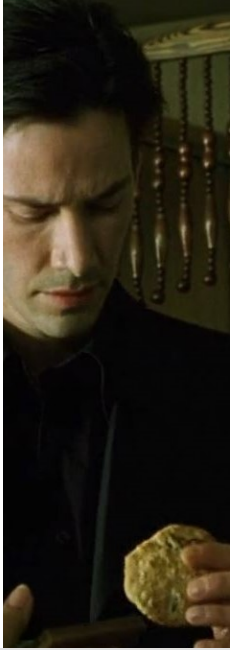
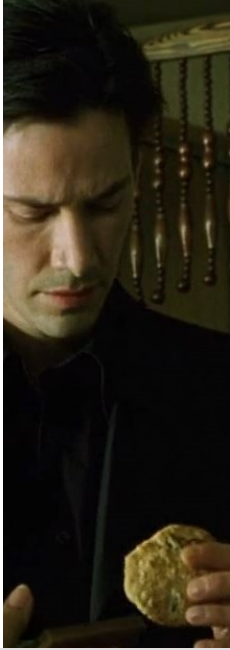


Tabla de contenidos



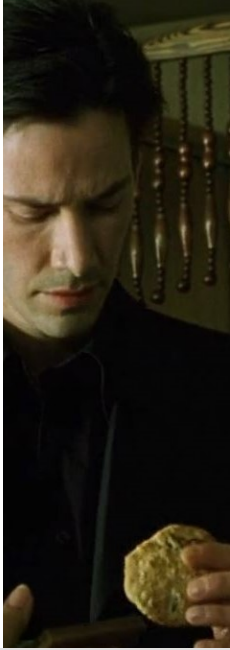
Artículo 3 - Aplicabilidad Extraterritorial del GDPR

- El GDPR se aplica a empresas fuera de la Unión Europea si:
  - Ofrecen bienes o servicios a ciudadanos de la UE
  - Realizan el monitoreo del comportamiento de ciudadanos europeos, aunque no se encuentren físicamente dentro de la UE
- Las empresas no europeas deben cumplir con las disposiciones del GDPR cuando:
  - Dirigen actividades comerciales hacia la UE (como la venta de productos o servicios)
  - Tratan datos de usuarios europeos, independientemente de si tienen una presencia física en la UE
- Las sanciones por el incumplimiento pueden ser severas, incluidas multas de hasta el 4



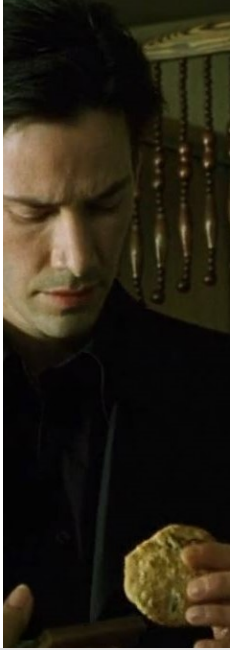
Relevancia del GDPR fuera de Europa

- El GDPR ha influenciado las legislaciones de privacidad en otros países, imponiendo estándares de protección de datos más estrictos
- Ejemplo notable: La Ley de Privacidad del Consumidor de California (CCPA), que establece derechos similares a los del GDPR, como el derecho a la información y a la eliminación de datos personales
- Empresas globales deben ajustar sus políticas y prácticas de protección de datos para garantizar el cumplimiento del GDPR, evitando sanciones que puedan afectar tanto a sus operaciones en la UE como a nivel global
- La implementación de estas regulaciones mejora la percepción de confianza y responsabilidad ante los usuarios, quienes se sienten más seguros con el tratamiento de sus datos personales



Ejemplos de Implementación Internacional

- Empresas estadounidenses como Google, Facebook y Amazon han ajustado sus plataformas y políticas de privacidad para cumplir con el GDPR, garantizando el tratamiento adecuado de los datos de los usuarios europeos
- En América Latina y Asia, países como Brasil (Lei Geral de Proteção de Dados - LGPD) y Japón han adoptado regulaciones similares al GDPR, enfocadas en la protección de datos personales y la privacidad de los ciudadanos
- Existe una creciente colaboración internacional para la estandarización de la privacidad, con esfuerzos conjuntos entre la UE, Estados Unidos, y otros países para crear marcos de protección de datos que sean interoperables y que eviten la fragmentación de regulaciones



¿Preguntas?

Fotografía de fondo:
https://connortumbleson.com/2018/01/28/understanding-the-matrix-triology/
Plantilla del tema:
https://github.com/ptoledo-teaching/pt-slides