informàTICs
Enginyers en informàtica de Catalunya

ISACA
Trust in, and value from, information systems

GDPR

DE LA TEORÍA A LA PRÁCTICA

Óscar Alonso Llombart
Information Strategist / Data Management & Analytics Knowledge Leader at everis
email: oalonsollombart@gmail.com / oscar.alonso.llombart@everis.com
mobile: +34 633 62 55 18
twitter: @oalonsollombart
linkedin: es.linkedin.com/in/oscaralonsollombart

Mireia Náger
Data Management & Analytics consultant at everis
email: mireia_nager@enginyeriainformatica.cat
linkedin: https://www.linkedin.com/in/mireianager/

1. Contexto
2. ¿Qué es GDPR?
3. El rol de la tecnología en GDPR
4. GDPR customer journey
5. Situación de las organizaciones

¿Por qué necesitamos una legislación de protección de datos?

¿Por qué necesitamos una legislación de protección de datos?

¿Qué es GDPR?

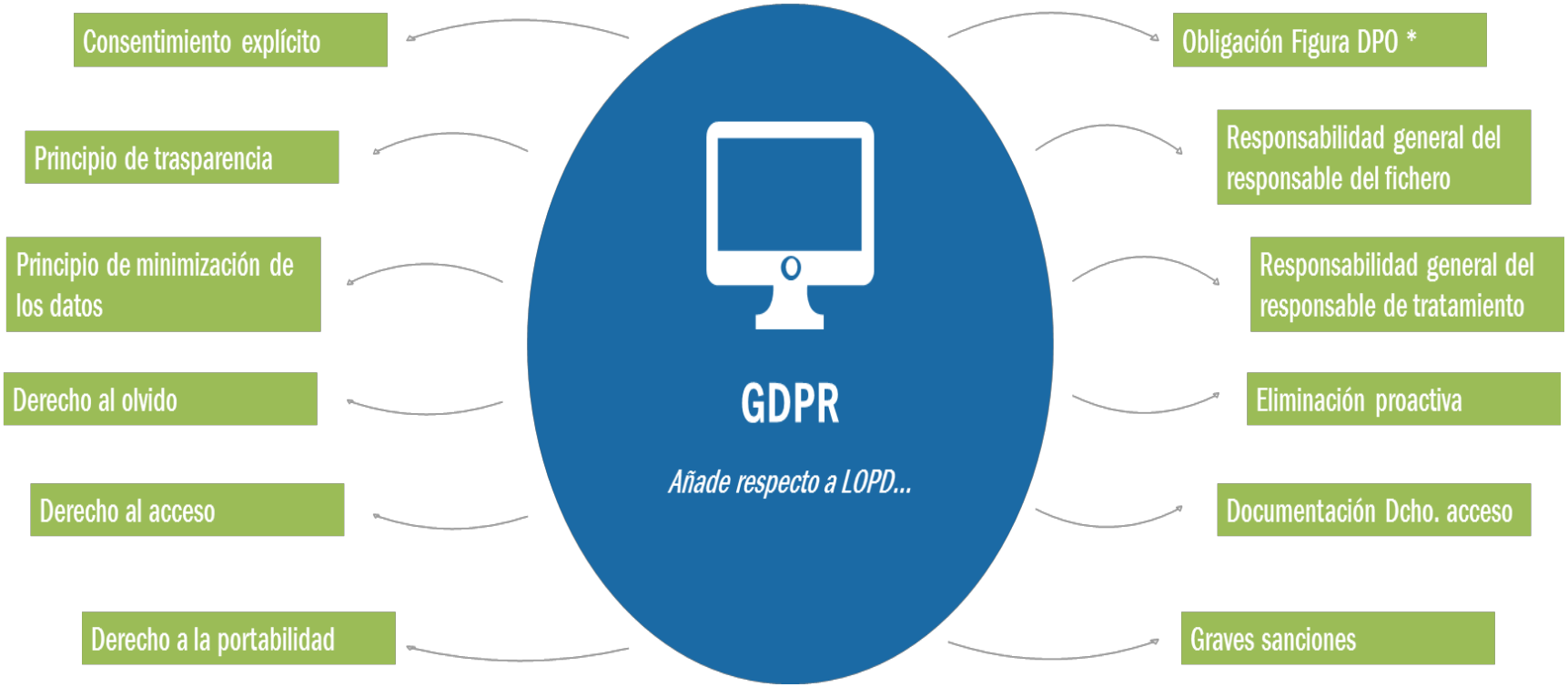
General Data Protection Regulation snapshot

Fuente: Council of the European Union – General Secretariat

General Data Protection Regulation snapshot

Fuente: Council of the European Union – General Secretariat

Cambios respecto la LOPD



* Obligación de contar con un DPO en organizaciones e instituciones públicas y en entidades con más de 250 trabajadores. En el caso de entidades con menos de 250 empleados, será obligatorio el DPO cuando necesiten un seguimiento sistemático y periódico de los datos personales tratados para la monitorización o investigación de mercados, análisis de riesgos o datos crediticios o de solvencia patrimonial, así como cuando traten los citados datos catalogados de especialmente protegidos

¿Cómo afecta el brexit?

Aunque la salida del Reino Unido de la Unión Europea implicará que el GDPR ya no será aplicable en dicho territorio, como esta salida no se producirá hasta pasado el plazo de aplicación del GDPR (25 de mayo de 2018), está previsto que las empresas se adecúen en dicho periodo

Este hecho fue confirmado verbalmente por Karen Bradley, Secretaria de Estado de Cultura, Medios de Comunicación y Deportes, el 24 de octubre de 2016 en el Comité de Cultura, Medios de Comunicación y Deportes

Aun así, las empresas que realicen tratamientos ya sea por cuenta propia o mediante terceros en alguno de los territorios del Reino Unido se enfrentan a una gran incertidumbre sobre si estos tratamientos serán legales una vez producido el “brexit”

“Brexit” con acuerdo sobre libre circulación de datos:

- Es posible que se produzca un acuerdo que implique la libre circulación de datos entre la UE y el Reino Unido
- Si se produce este acuerdo, las empresa del Reino Unido deberán cumplir con el GDPR y no habrá diferencia entre un tratamiento llevado a cabo en Portugal o en Inglaterra, no existiendo transferencial internacional de datos

“Brexit” sin acuerdo pero con normativa:

- Se produce la salida sin acuerdo, pero el Reino Unido decide adoptar el GDPR como una norma interna. Se considera transferencia internacional
- Esto colocaría al Reino Unido en la posición de obtener una Decisión de la Comisión declarando que el Reino Unido garantiza un nivel de protección adecuado
- Para la realización de transferencias no será necesario obtener ninguna autorización específica

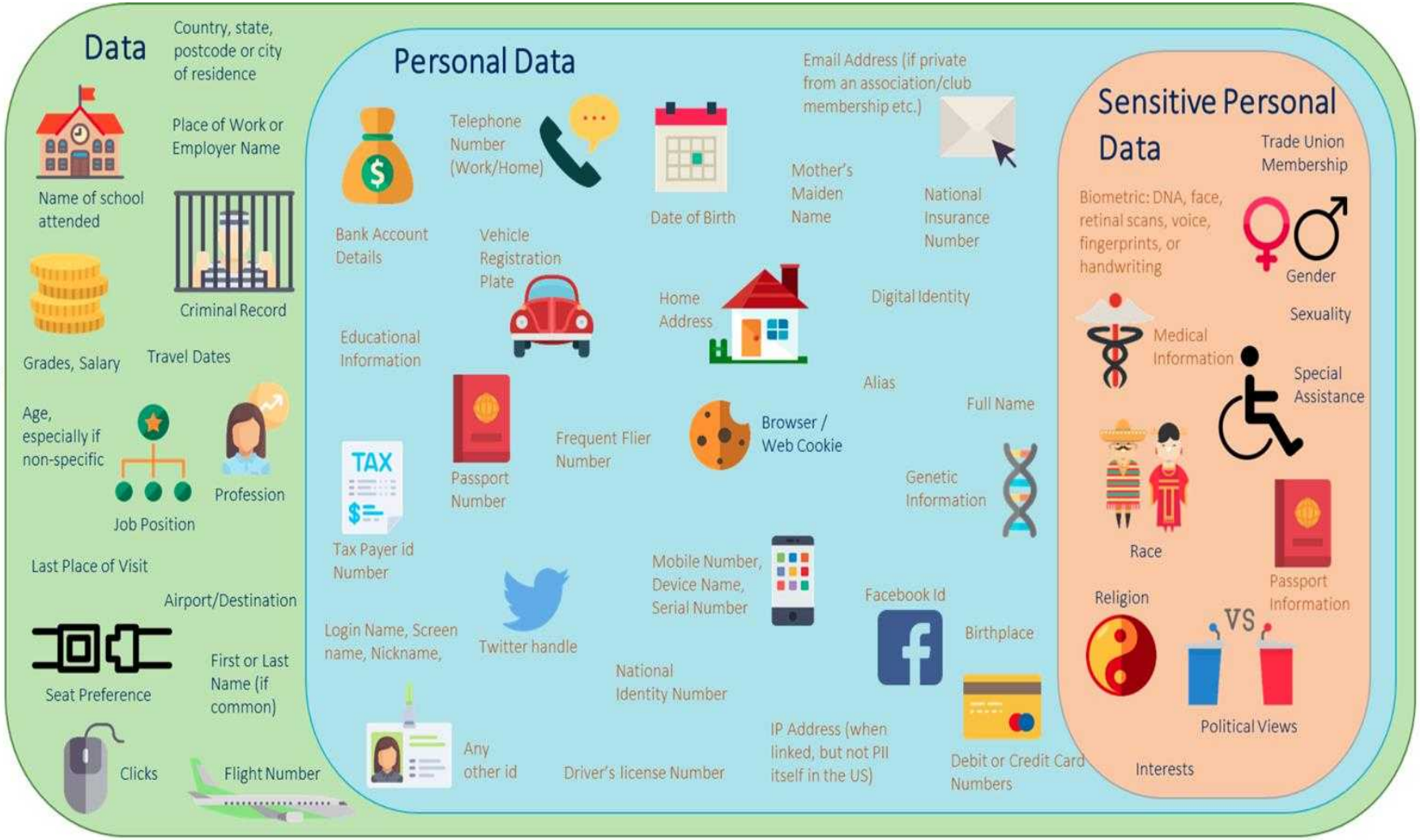
¿Cómo afecta el brexit?

“Brexit” sin acuerdo y sin normativa:

- Es el peor escenario ya que las transferencias internacionales no podrán ser automáticas como en los supuestos anteriores. Para poder realizar las transferencias será necesario adoptar alguno se los siguientes esquemas:
  - ❖ Transferencia mediante garantías adecuadas sin necesidad de autorización por parte de la AEPD:
    - o mediante la firma de normas corporativas vinculantes cuando son empresas del mismo grupo empresarial,
    - o la firma de un acuerdo siguiendo el clausulado establecido por la autoridad de control o por la Comisión,
    - o por la obtención de una certificación o la adhesión a un código de conducta de los establecidos en el GDPR
  - ❖ Transferencia mediante garantías adecuadas con autorización por parte de la AEPD cuando se haya suscrito un acuerdo sin las cláusulas tipo.
  - ❖ El interesado haya prestado su consentimiento explícito
  - ❖ Sea necesaria para la ejecución de un contrato suscrito por el interesado o en interés de interesado
  - ❖ Por razones importantes de interés público
  - ❖ Para la formulación, el ejercicio o la defensa de reclamaciones
  - ❖ Para proteger los intereses vitales del interesado o de otras personas
- En caso de no estar en uno de los supuestos anteriores no se podrá realizar la transferencia internacional al Reino Unido

"**personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly (…), in particular by reference to an identifier such as a **name**, an i**dentification number**, **location data**, **online identifier** or to **one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity** of that person"

Datos personales contemplados



Principios fundamentales de GDPR

1. **‘<u>lawfulness, fairness and transparency</u>’ -** processed lawfully, fairly and in a transparent manner in relation to the data subject.

2. **‘<u>purpose limitation</u>’ -** collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. **‘<u>data minimisation</u>’ -** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

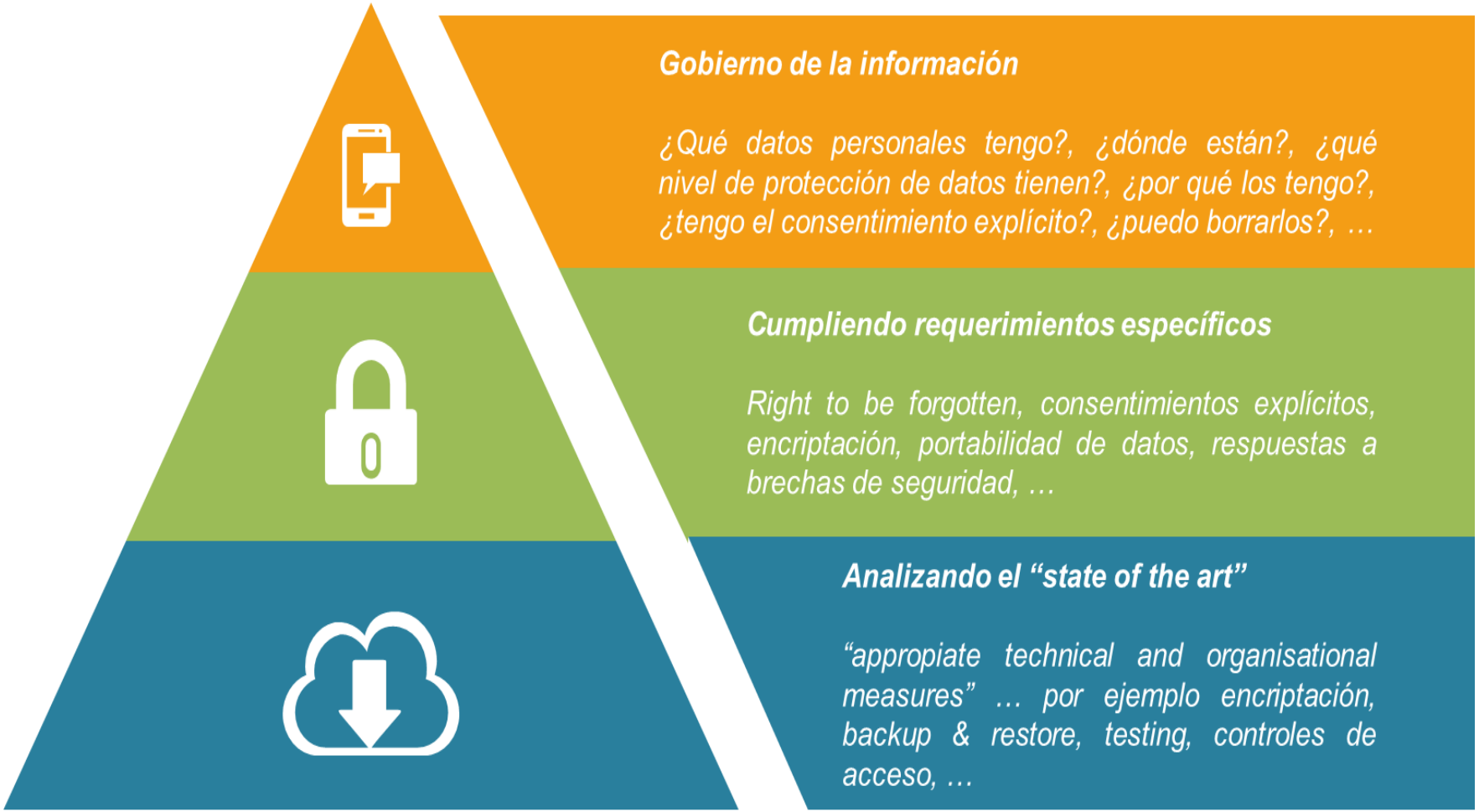
4. **‘<u>accuracy</u>’ -** accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

5. **‘<u>storage limitation</u>’ -** kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

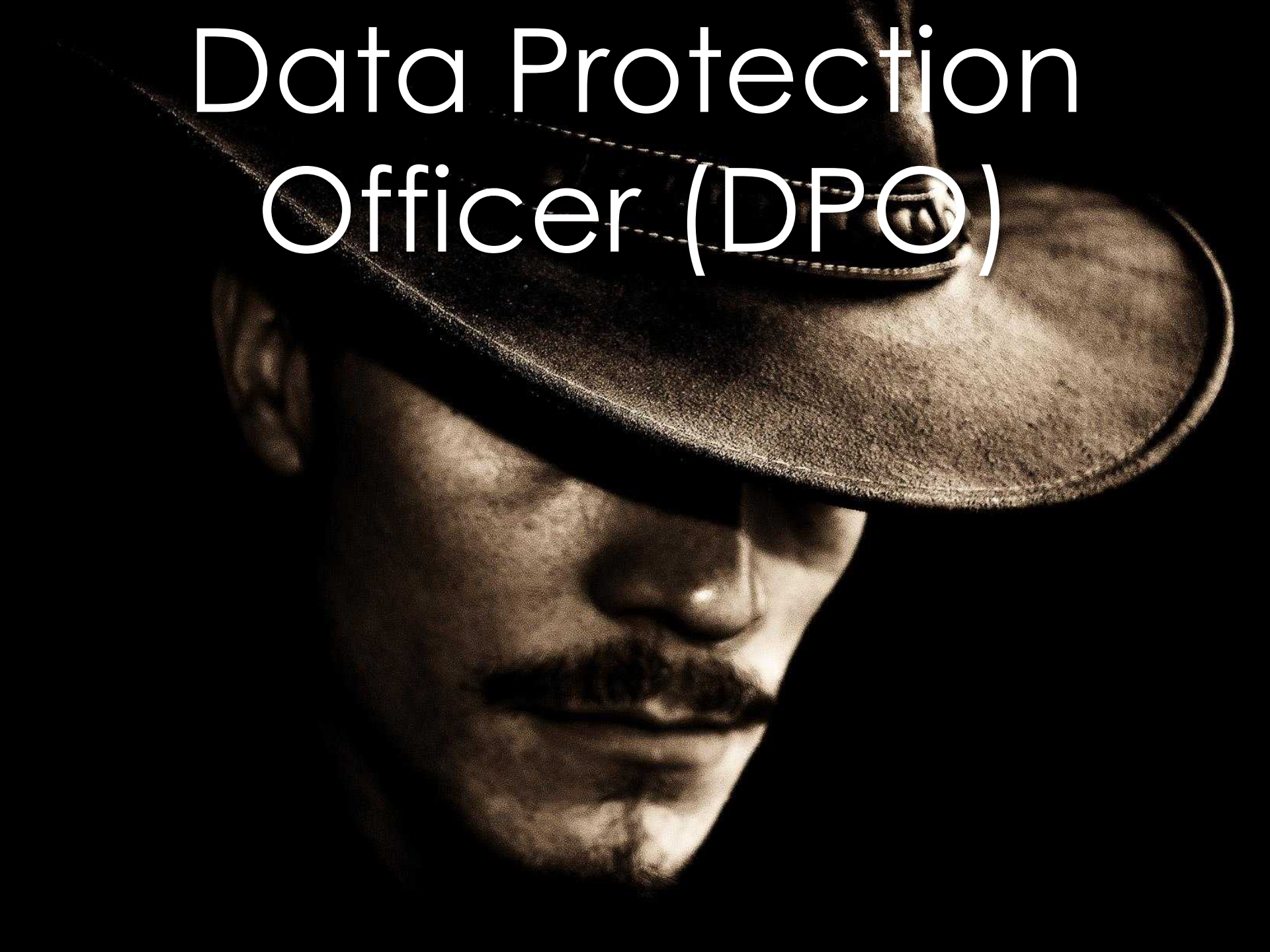
6. **‘<u>integrity and confidentiality</u>’ -** processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss destruction or damage, using appropriate technical or organisational measures.

7. **’<u>accountability</u>’** – refers generally to the various obligations organizations will have to follow in order to demonstrate data protection compliance

El rol de la tecnología en GDPR



Data Protection Officer (DPO)

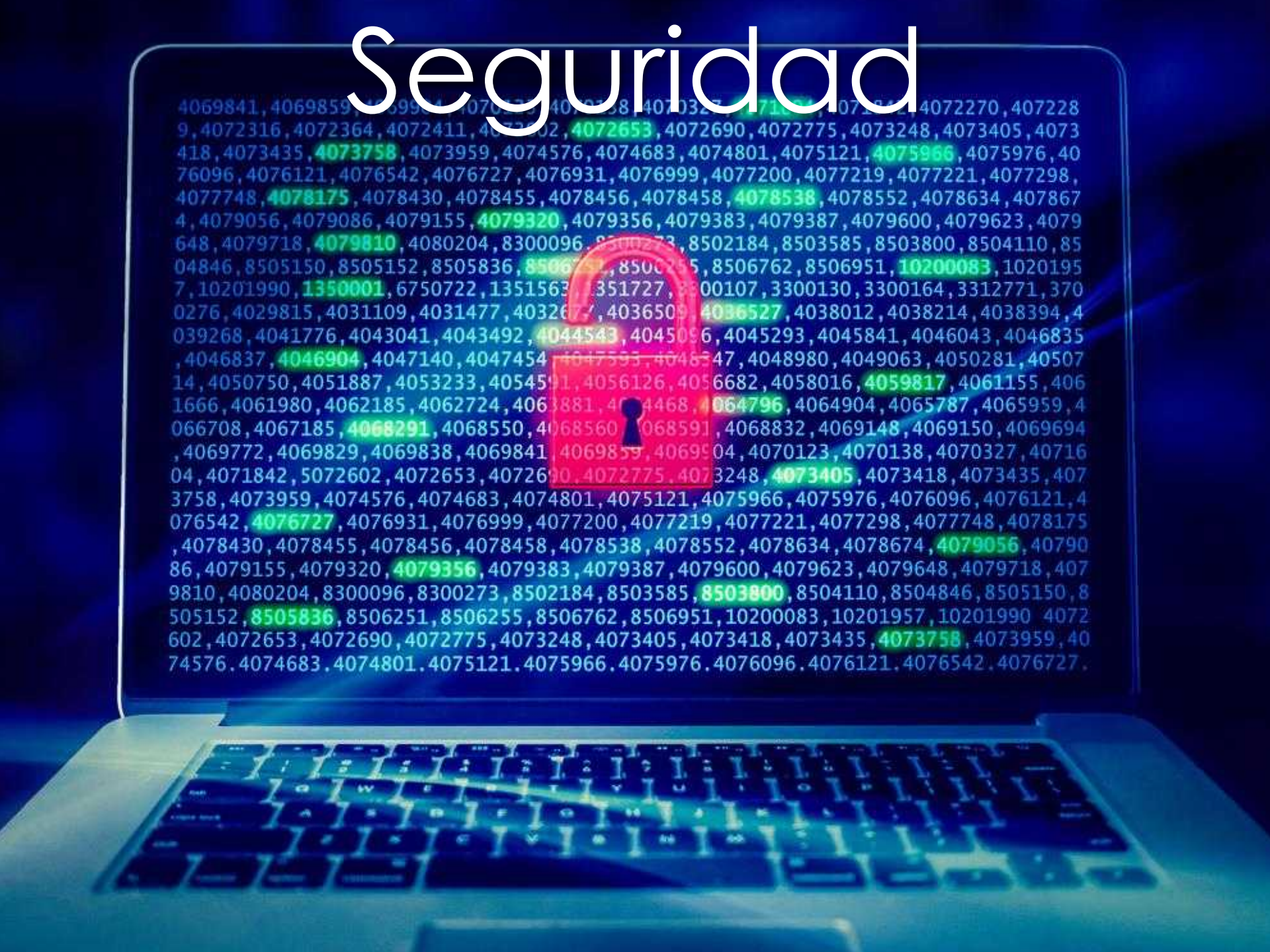


CDO & DPO

Privacy Impact Assessments (PIAs)

Responsabilidad proactiva y gobierno de la información

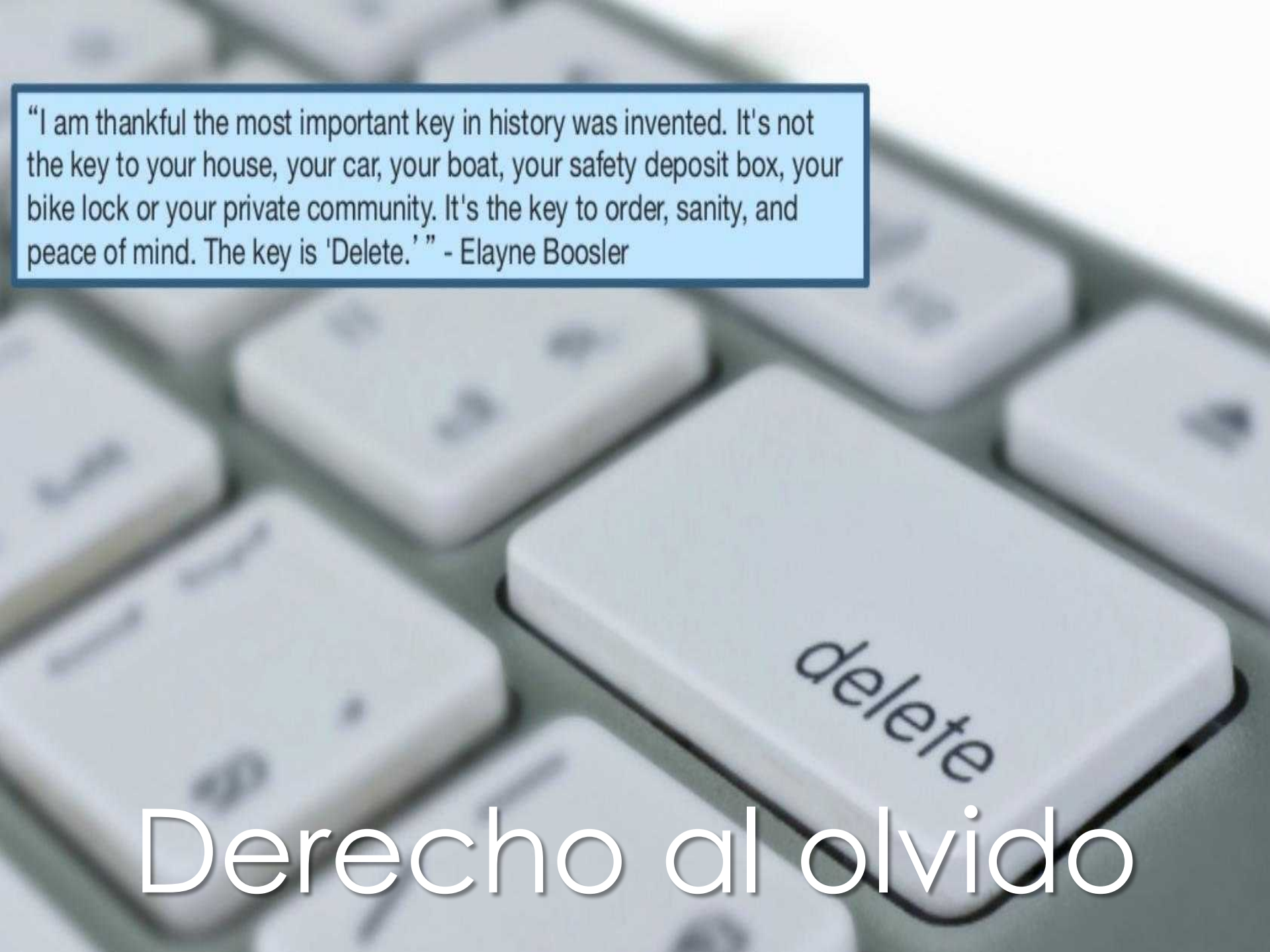
Seguridad



Derecho a la información

Derecho a la rectificación

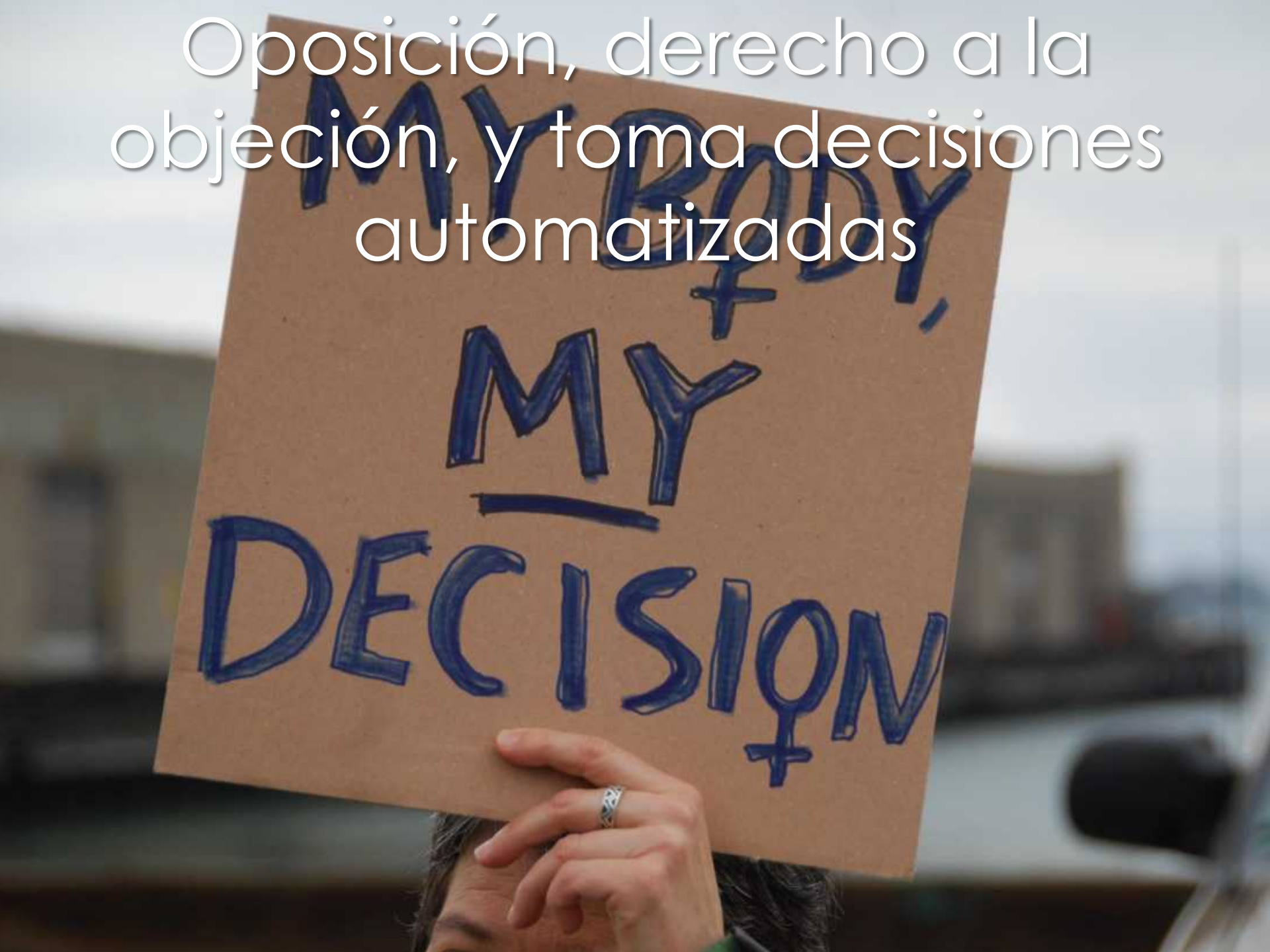
Derecho a la portabilidad



"I am thankful the most important key in history was invented. It's not the key to your house, your car, your boat, your safety deposit box, your bike lock or your private community. It's the key to order, sanity, and peace of mind. The key is 'Delete.' " - Elayne Boosler

Derecho al olvido

Oposición, derecho a la objeción, y toma decisiones automatizadas



GDPR Customer Journey

	NECESIDAD	COMPRA	USO	CANCELACIÓN
	• NAVEGAR EN LA WEB • IR DE COMPRAS • RESOLVER DUDAS	• REGISTRO ONLINE • REALIZAR COMPRA • SUBSCRIPCIÓN A SERVICIOS	• UTILIZAR EL SERVICIO O PRODUCTO • RECLAMACIONES • FEEDBACK	• CANCELAR SUBSCRIPCIÓN
	• MARKETING • MARKETING ONLINE • SOPORTE A LA COMPRA	• ALTA CLIENTE • ALTA SERVICIO • ENVÍO DE PRODUCTO	• PRESTACIÓN DE SERVICIO • ATENCIÓN AL CLIENTE • PROMOCIONES • FIDELIZACIÓN	• BAJA EN LOS SISTEMAS • ANÁLISIS BAJA

CHANNELS

GESTIÓN DE CONSENTIMIENTOS	INFORMACIÓN Y ACCESO A DATOS PERSONALES	EJERCICIO DE DERECHOS	NOTIFICACIÓN DE BRECHAS

Seguridad de la información

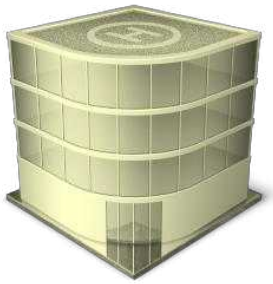
Gobierno responsable

Principales actores

CIUDADANO

(clientes)
(empleados)
(subcontratados)
(candidatos)
(afiliados)
(…)

RESPONSABLE
DEL TRATAMIENTO



ENCARGADO
DEL TRATAMIENTO

AUTORIDAD
DE CONTROL

Gestión de consentimientos

NECESIDAD	COMPRA	USO	CANCELACIÓN
• COOKIES • NEWSLETTER Y MARKETING ONLINE	• REGISTRO CLIENTE	• PERFILADO DE CLIENTES • NUEVOS TRATAMIENTOS	• REVOCACIÓN

EL CONSENTIMIENTO DEBE SER:

- AFIRMATIVO
- LIBRE
- ESPECÍFICO
- INFORMADO
- INEQUIVOCO

NIÑOS +16 (*)

Y ES NECESARIO PODER DEMOSTRAR QUE SE HA OBTENIDO!

Ejemplo:

☐ **Marcando esta casilla, acepto y reconozco haber leído las** Condiciones Generales de Venta de Fnac.es **y las** Condiciones Generales de Venta de MarketPlace

https://secure.fnac.es/account/register

Información

NECESIDAD → COMPRA → USO → CANCELACIÓN

Se debe **informar siempre de los tratamientos**, tanto si los datos son obtenidos del interesado como por otras vías.

La información necesaria es:

- ✓ Identidad y datos de contacto del responsable
- ✓ Datos de contacto del DPO
- ✓ Finalidad
- ✓ Legitimación
- ✓ Destinatarios
- ✓ Transferencias internacionales
- ✓ Plazo de conservación
- ✓ Existencia de decisiones automatizadas, lógica aplicada, importancia y consecuencias
- ✓ Derechos

NOMBRE DEL PORVEEDOR	FINALIDAD DE LA COOKIE	DESCRIPCIÓN DE LA FINALIDAD DE LA COOKIE	SI DESEA MÁS INFORMACIÓN SOBRE EL USO DE LAS COOKIES DE ESTE TERCERO
ScorecardResearch	Analíticas	Tiempo de navegación, sitio web visitado e información relacionada con la propia navegación.	http://www.scorecardresearch.com/privacy.aspx
AddThis	Analíticas	Cuando los vínculos se proporcionan a los servicios de terceros que encuentras útiles, puedes colocar una cookie en tu dispositivo para realizar tu servicio más fácil de usar. Esta cookie te permite compartir contenidos a través de estas páginas Web y del correo electrónico.	http://support.addthis.com/
Google	Publicidad	Doubleclick es usado para gestionar las cookies de terceros. Estas cookies son usadas para proveer a los usuarios de productos relevantes que pueden ser de interés para el usuario. Los anuncios que ven los usuarios de la página web son atendidos por una pequeña selección de proveedores, incluyendo Invitemedia, Adviva.net, MSN, Google Display and Unanimis.	http://www.google.com/doubleclick/
Google	Analíticas	Cookies de Google Analytics. Generan un ID de usuario anónimo, que es el que se utiliza para hacer recuento de cuantas veces visita el sitio un usuario. También registra cuando fue la primera y la última vez que visitó la web. Asimismo, calcula cuando se ha	https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage

http://www.elcorteingles.es/cookies/

Y cuando no se obtengan del interesado, además se necesitarán las **categorías de datos personales** y la **fuente de la que proceden**.

Información

Sensitive personal details relating to almost 200 million US citizens have been accidentally exposed by a marketing firm contracted by the Republican National Committee.

BBC news, 19 Junio 2017
http://www.bbc.com/news/technology-40331215

Un fichero con datos de 36 millones de españoles reúne 5 millones en multas

El archivo viola desde hace cuatro años la ley de Protección de Datos

El País, 19 Dec 2011
http://sociedad.elpais.com/sociedad/2011/12/18/actualidad/1324239911_364530.html

Ejercicio de derechos

Solicitud

Resolución

MEDIDAS TÉCNICAS Y ORGANIZATIVAS

CANALES DE COMUNICACIÓN DERECHOS

GESTIÓN DATOS PERSONALES

REPOSITORIOS

- SISTEMAS TRANSACCIONALES
- DWH
- SISTEMAS DE FICHEROS
- DISPOSITIVOS
- REPOSITORIOS FÍSICOS
- ARCHIVO
- ...

GESTIÓN DE CONSENTIMIENTOS

DERECHO DE ACCESO

DERECHO A RECTIFICACIÓN

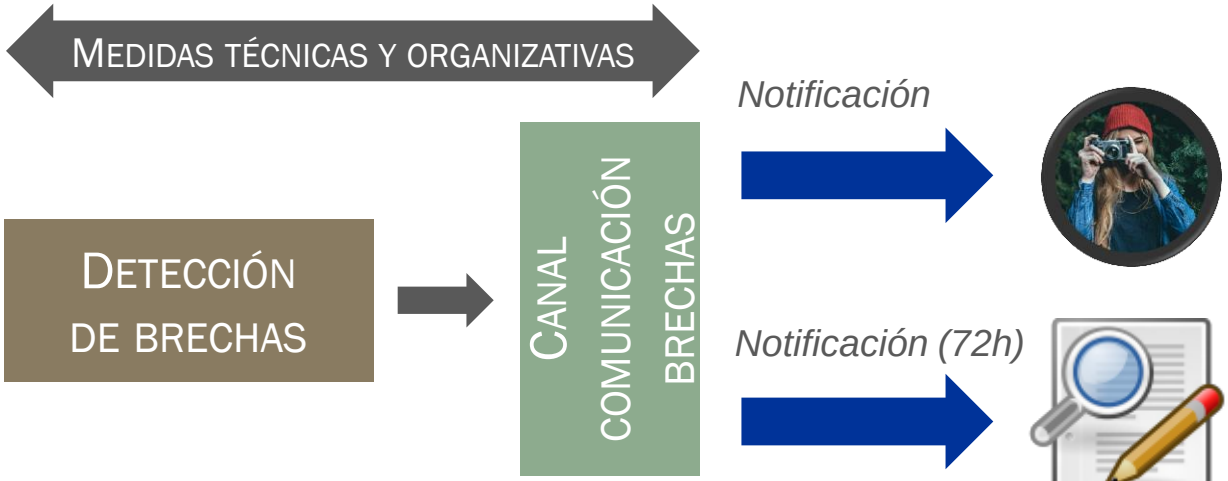
DERECHO DE SUPRESIÓN

DERECHO A LA PORTABILIDAD

DERECHO A LA LIMITACIÓN DE TRATAMIENTO

DERECHO A OPOSICIÓN

Notificación brechas de seguridad



La notificación incluye:

- ✓ *DPO*
- ✓ *Posibles consecuencias*
- ✓ *Medidas correctivas adoptadas o propuestas*

Y a la autoridad, además:

- ✓ *Naturaleza de la brecha*
- ✓ *Categorías y número de registros*
- ✓ *Número de afectados*

Medidas organizativas: *Formación y concienciación de toda la organización:*

- *Situaciones en las que sucede una brecha de seguridad*
- *Protocolos de actuación en caso de brechas de seguridad*

Medidas técnicas: *Establecer medidas de detección automática mediante la monitorización y detección de patrones en diferentes ámbitos:*

- *Accesos y operaciones sobre la información personal*
- *Logs de los diferentes elementos de la infraestructura*

Brechas de seguridad

Qué son?

- ✓ Destrucción, pérdida o alteración accidental o ilícita de datos personales
- ✓ Comunicación o acceso no autorizado a datos personales accidental

Hasta 3.000 euros de multa por olvidar poner los e-mails en copia oculta

La Vanguardia, 9 Jul 2010
http://www.lavanguardia.com/internet/20100709/53959370636/hasta-3-000-euros-de-multa-por-olvidar-poner-los-e-mails-en-copia-oculta.html

Economía.- La Agencia Española de Protección de Datos multa a Worten por vender un disco duro ya usado

La Agencia Española de Protección de Datos (AEPD) ha multado a Worten con 10.000 euros tras haber vendido a un cliente como producto nuevo un disco duro ya usado, y en cuyo interior además se encontraban almacenados datos personales de todos los empleados de la empresa, según ha informado Facua en un comunicado.

La Vanguardia, 10 Agosto 2016
http://www.lavanguardia.com/vida/20160810/403828133999/economia--la-agencia-espanola-de-proteccion-de-datos-multa-a-worten-por-vender-un-disco-duro-ya-usado.html

ROBO DE DATOS ›

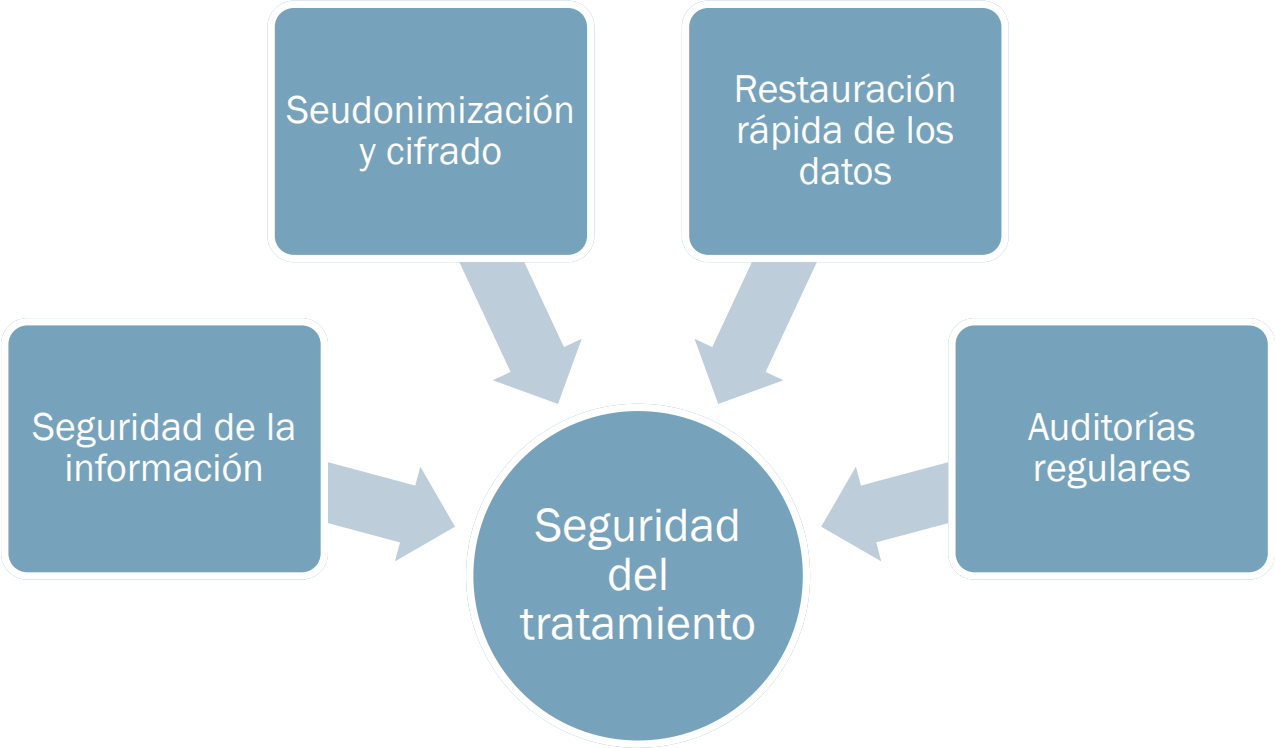
Yahoo anuncia el robo de datos de mil millones de cuentas

La compañía admite un nuevo hackeo, que dobla el que reveló hace solo tres meses

El País, 15 Dec 2016
http://tecnologia.elpais.com/tecnologia/2016/12/14/actualidad/1481753868_540005.html

Seguridad del tratamiento

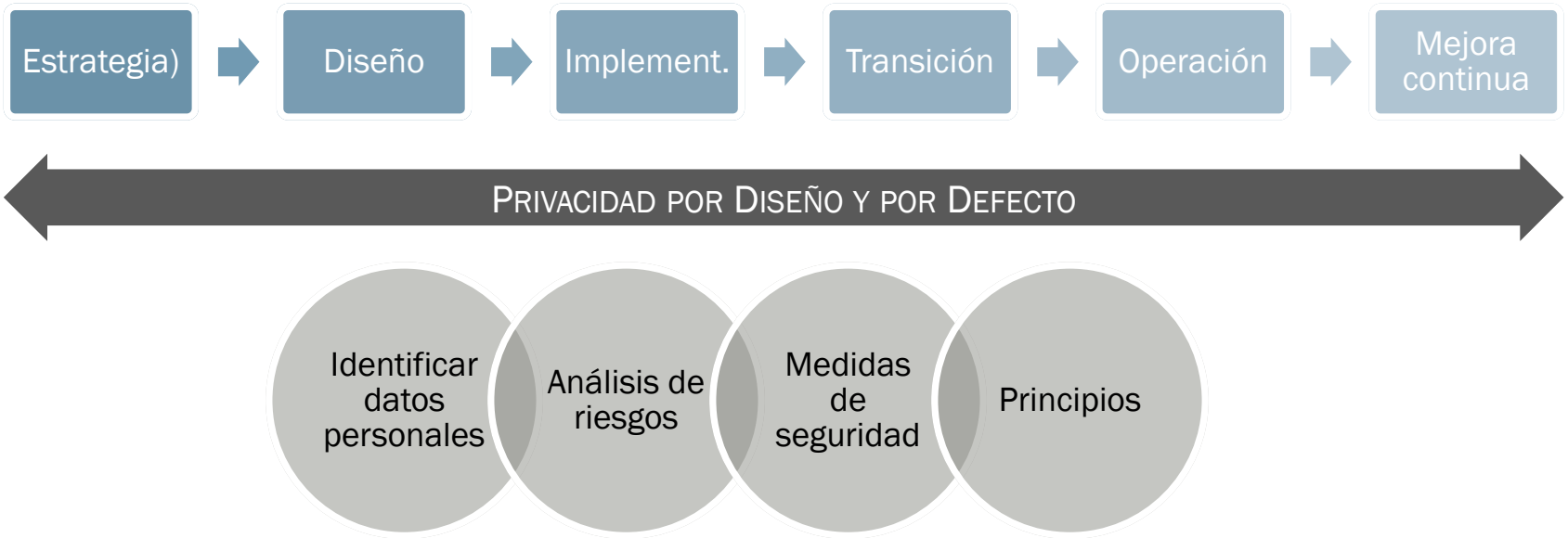
Se definirá un nivel de seguridad adecuado al riesgo y gravedad de los datos que se gestionan



Privacy by design and by default

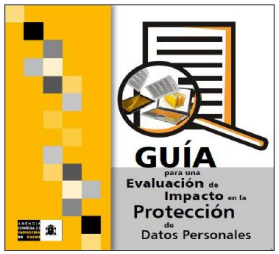
By Design: Incluir en los proyectos y servicios que sustentan los procesos de negocio de la compañía la gestión de la privacidad de los datos durante todo el ciclo de implementación.

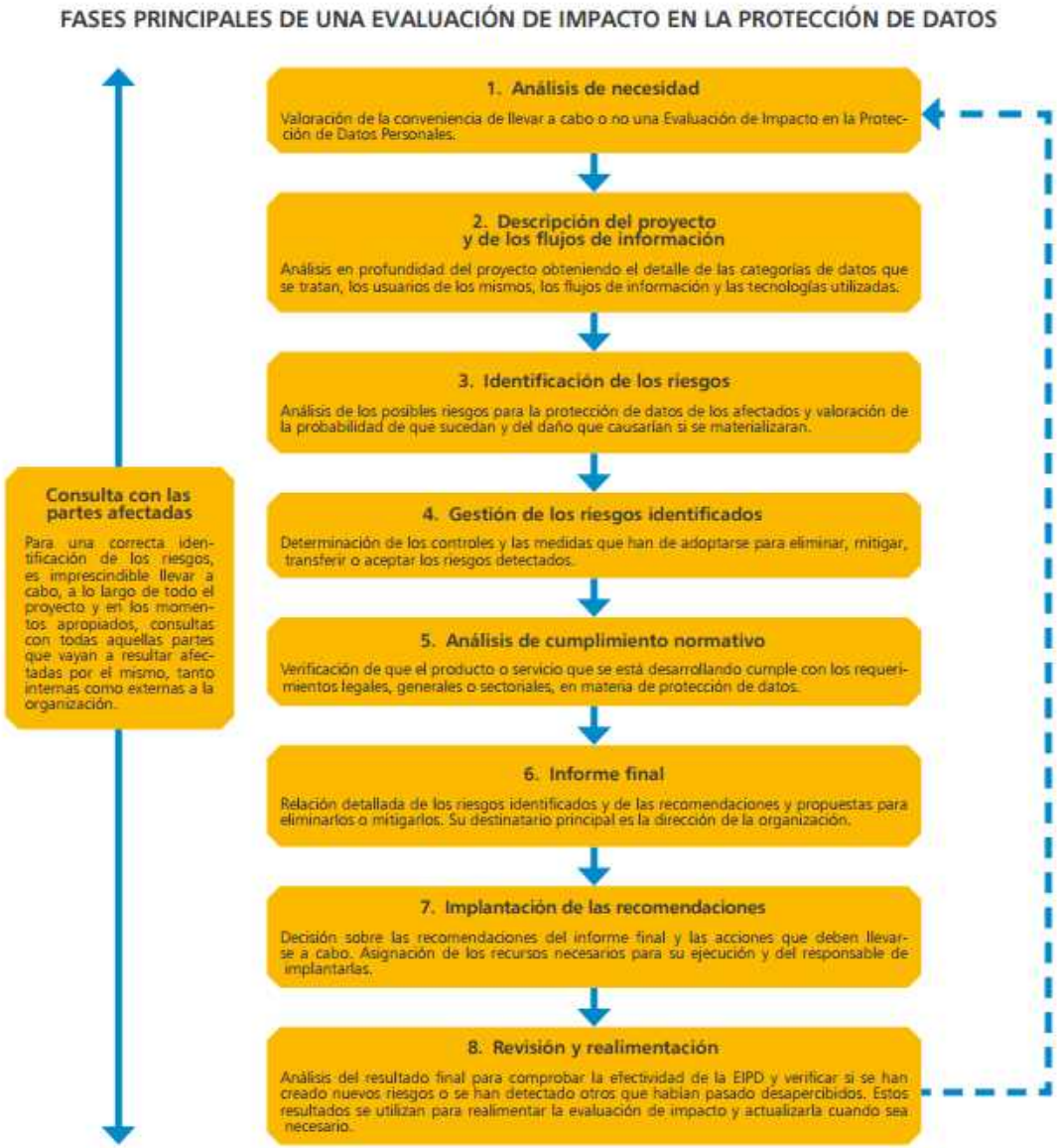
By default: Por defecto, la configuración será lo más limitada y restringida posible: permisos de acceso, información almacenada, etc.



DPIA

Cuando el tratamiento conlleva **elevado riesgo** para los derechos y libertades de los ciudadanos se ha de realizar una **evaluación de impacto/riesgos de datos personales.**



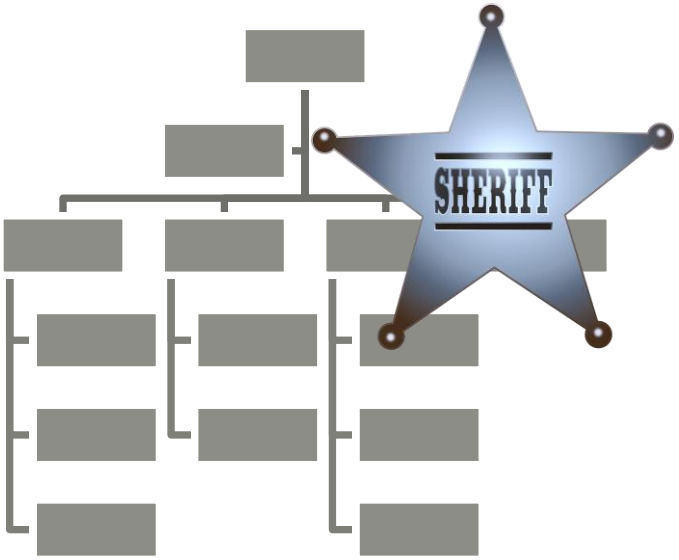


https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

Principios

Limitación del plazo de conservación
Integridad y confidencialidad
Lícitud, lealtad y transparencia
Limitación de la finalidad
Minimización de datos
Exactitud

Gobierno responsable



Responsabilidad proactiva: Cumplimiento y demostración de los principios en todos los tratamientos llevados a cabo en la organización.

Concienciación e implementación de medidas de protección de datos en toda la organización

Asignación de un DPO

- Informar y asesorar
- Supervisar el cumplimiento
- Ofrecer asesoramiento en evaluaciones de impacto
- Cooperar y actuar como punto de contacto con la autoridad de control

Gobierno responsable

Códigos de conducta y certificación

- Con el objetivo de contribuir a la correcta aplicación de GDPR

Registro de actividades de tratamiento

- Responsable y encargado del tratamiento guardarán el registro

Transferencias internacionales

- Las transferencias internacionales deben proporcionar garantías de un nivel de protección adecuado

Registro de actividades de tratamiento

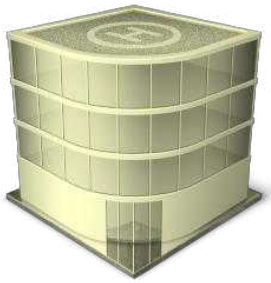
Responsable	Encargado
Datos contacto responsable Datos de contacto DPO Fines del tratamiento Interesados Datos personales Destinatarios Transferencias Plazos de supresión (*) Medidas de seguridad (*)	Datos contacto encargado Datos de contacto DPO Datos contacto responsable Tratamientos Transferencias Medidas de seguridad (*)

(*) Cuando sea posible

Responsable vs encargado

RESPONSABLE
DEL TRATAMIENTO

- Garantiza que el tratamiento cumple la regulación
- Aplica políticas de protección de datos adecuadas



ENCARGADO
DEL TRATAMIENTO

- Sigue las instrucciones documentadas del responsable
- Ofrece garantías de aplicación de medidas de protección adecuadas
- No recurrirá a otro encargado sin autorización escrita del responsable
- Existe un contrato responsable-encargado donde se definirán los detalles del tratamiento
- Pondrá a disposición del responsable la información necesaria para demostrar el cumplimiento

La adhesión a códigos de conducta o certificación ayuda a garantizar el cumplimiento por ambas partes

Cómo empezar un proyecto GDPR?

1. Conoce la organización e identifica los puntos débiles en el tratamiento de datos personales

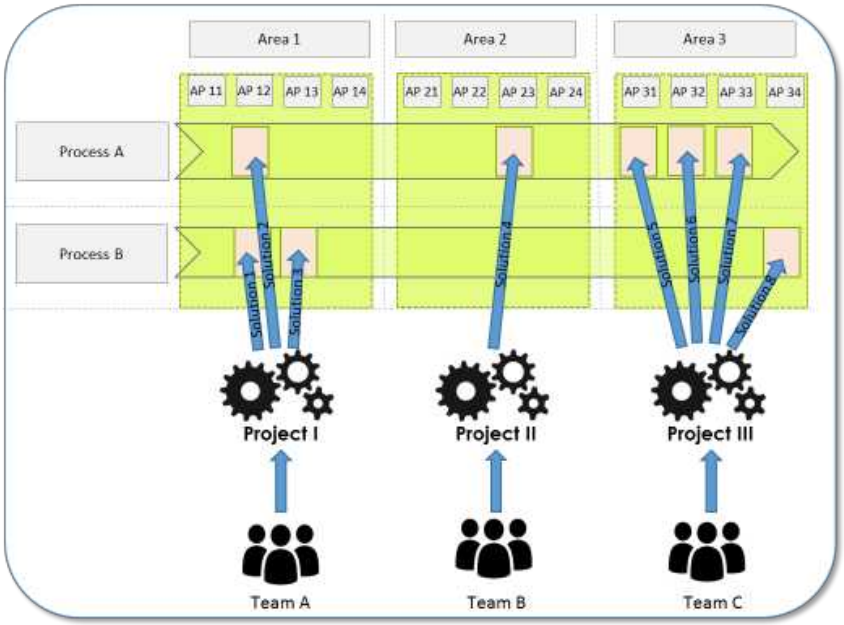
2. Crea un inventario de datos personales y tratamientos si no existe e identifica a las personas clave que se deben involucrar en el proceso

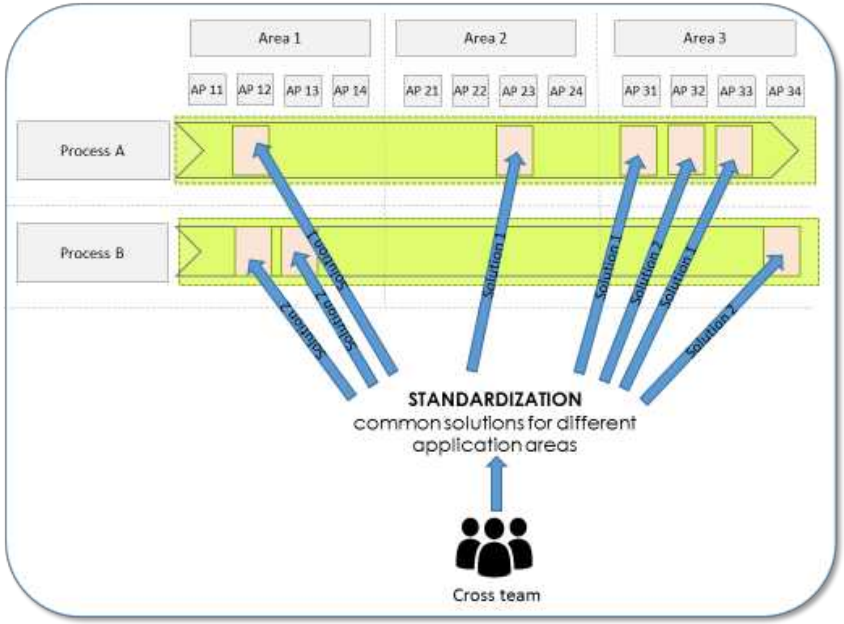
3. Define las medidas técnicas y organizativas a aplicar en la organización así como el enfoque metodológico

4. Implementa las medidas definidas para la adaptación a la nueva regulación

5. Formación y concienciación de todo el personal en la organización

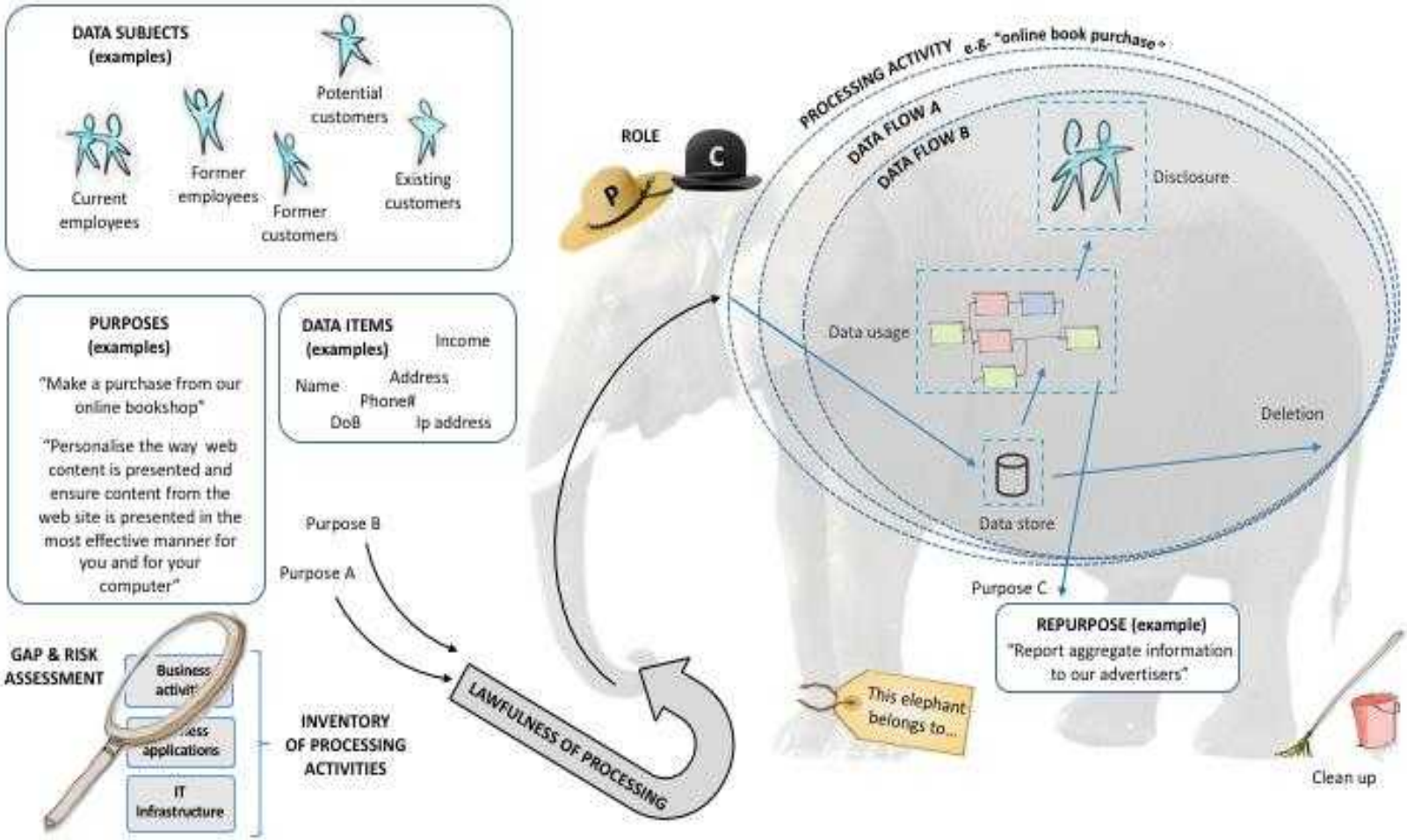
Cómo empezar un proyecto GDPR?





Estandarización o aplicación por área?

El propósito como punto de partida



Fuente: Tim Clements

Retos

La privacidad de los datos desde sus restricciones de diseño, seguridad y tecnología impactan en la soluciones end-to-end

Limitaciones en las infraestructuras actuales

Inconsistencias en formatos de datos, protocolos y documentación para el cumplimiento

Dificultades de armonización de los datos en industrias y entre entidades. Mentalidad de “silos” a nivel departamental con los sistemas y formatos de los datos

Los plazos “fuerzan” a las organizaciones a implantar soluciones tácticas en lugar de estratégicas, causando problemas a medio-largo plazo

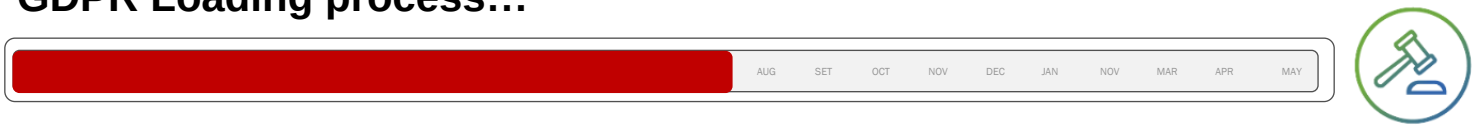
Limitaciones presupuestarias para el cumplimiento de GDPR y su mantenimiento sostenible

Situación de las organizaciones

"Research results from the Global Databerg Report, which involved more than 2,500 leading technology authorities in 2016 in Europe, the Middle East, Africa, the United States and Asia Pacific, reveal that **54% of organizations have not made progress in its preparation to comply with GDPR"**

The Global Databerg Report, 2016

GDPR Loading process…



Hoy
2017, Julio

Deadline
2018, 25 de Mayo

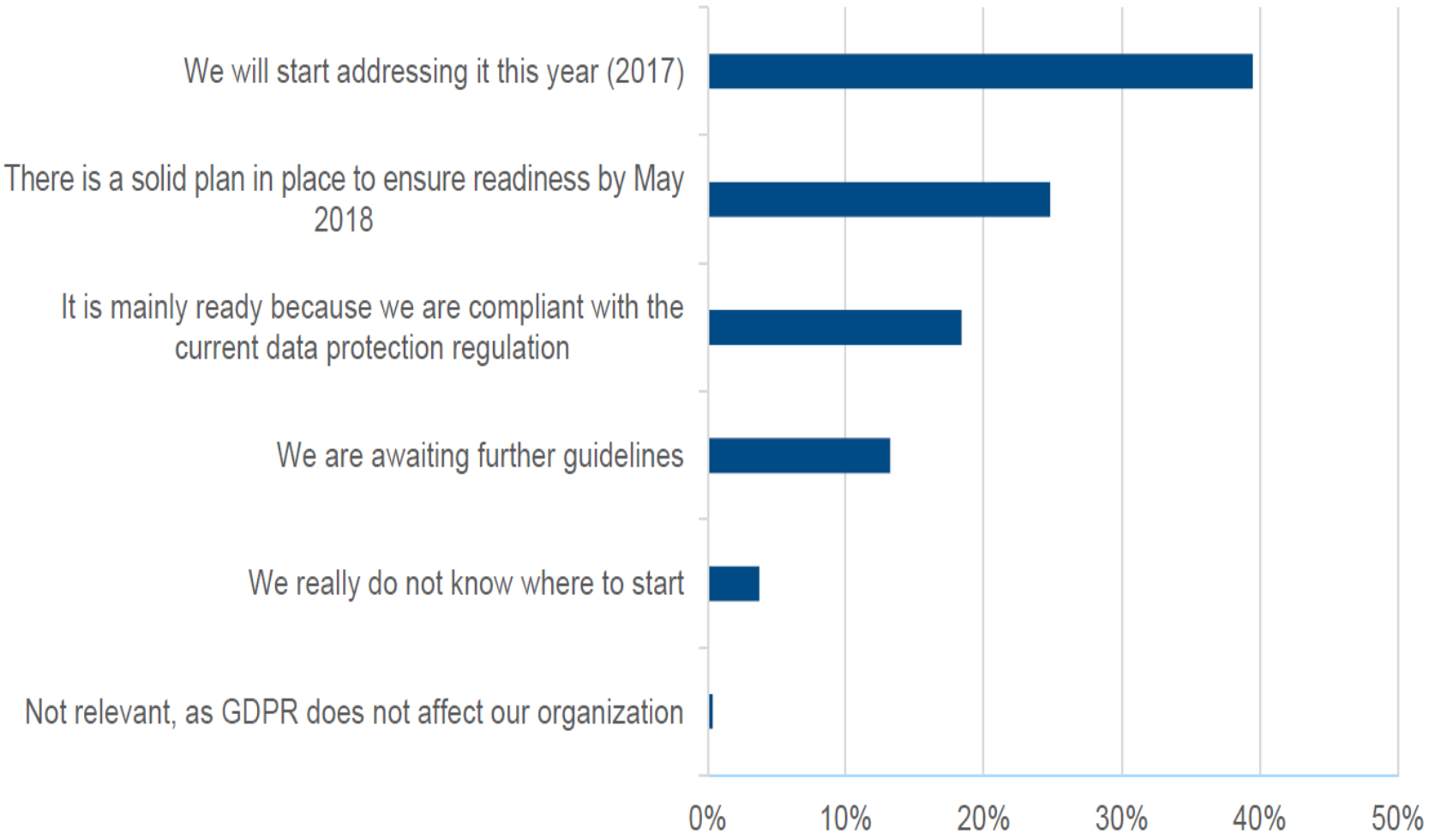
"By the **end of 2018, over 50% of companies affected by the GDPR will not be in full compliance** with its requirements"

Gartner, 2016

"Recent research into how companies were preparing for the GDPR across the U.S. and Europe showed half of companies were still unaware of the changes, while others were investing up to $0.5 million to address the new law. **55% of companies surveyed were looking for more detailed guidance on the GDPR and 43% were looking for technology solutions** to meet the new compliance requirements"

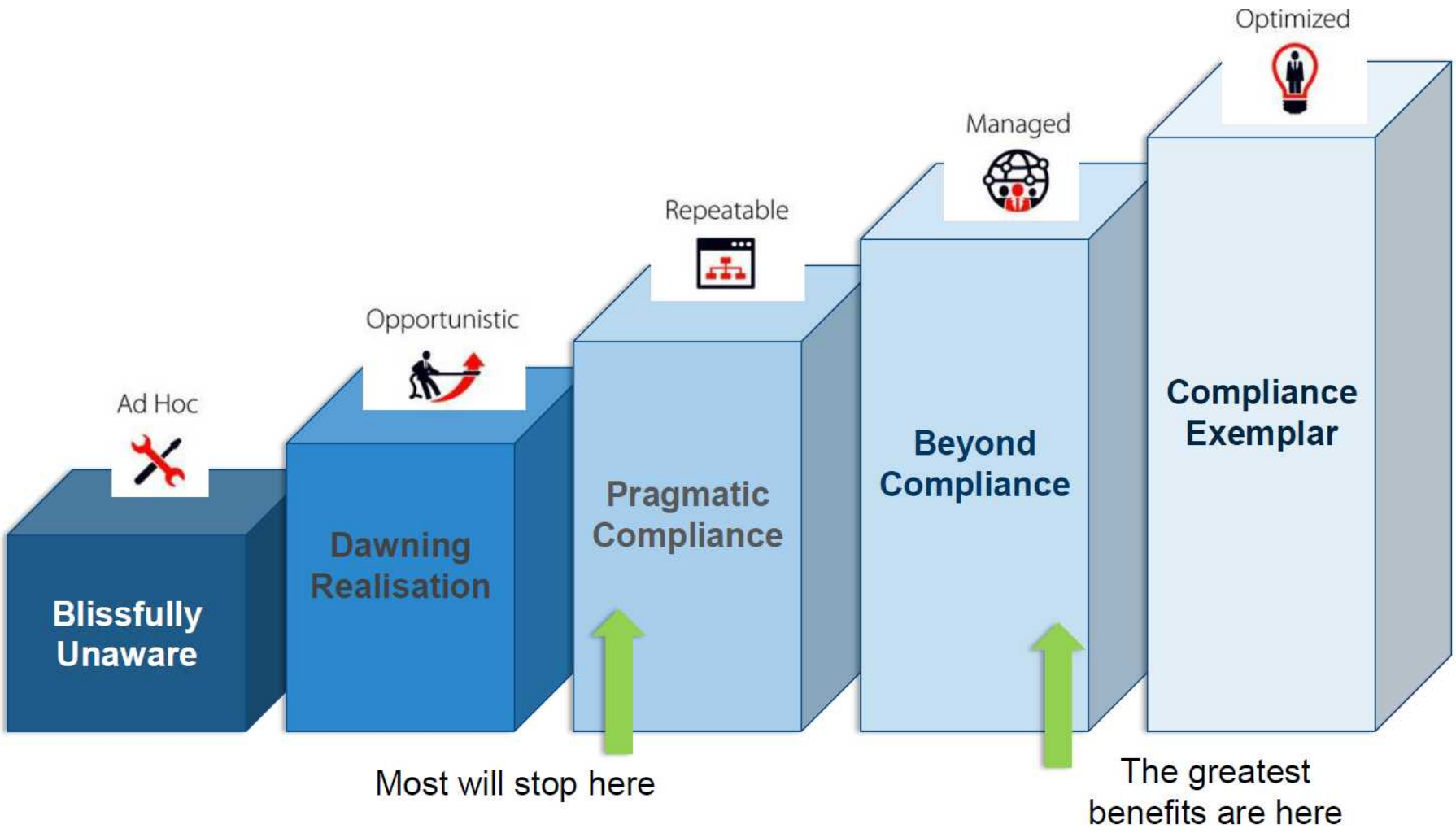
PRNewswire, 2015

Situación de las organizaciones



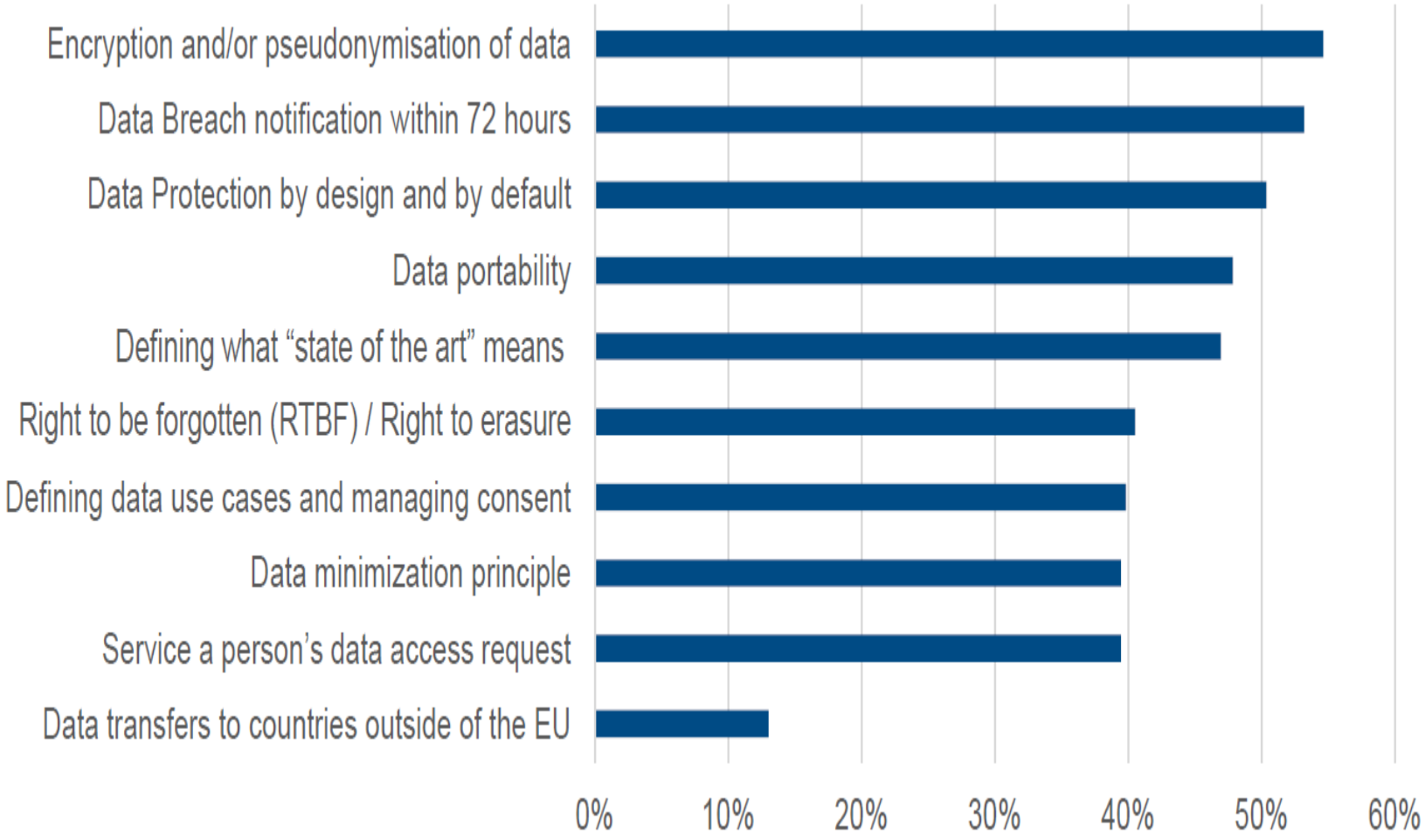
Fuente: IDC's 2017 GDPR survey, n=560

Situación de las organizaciones



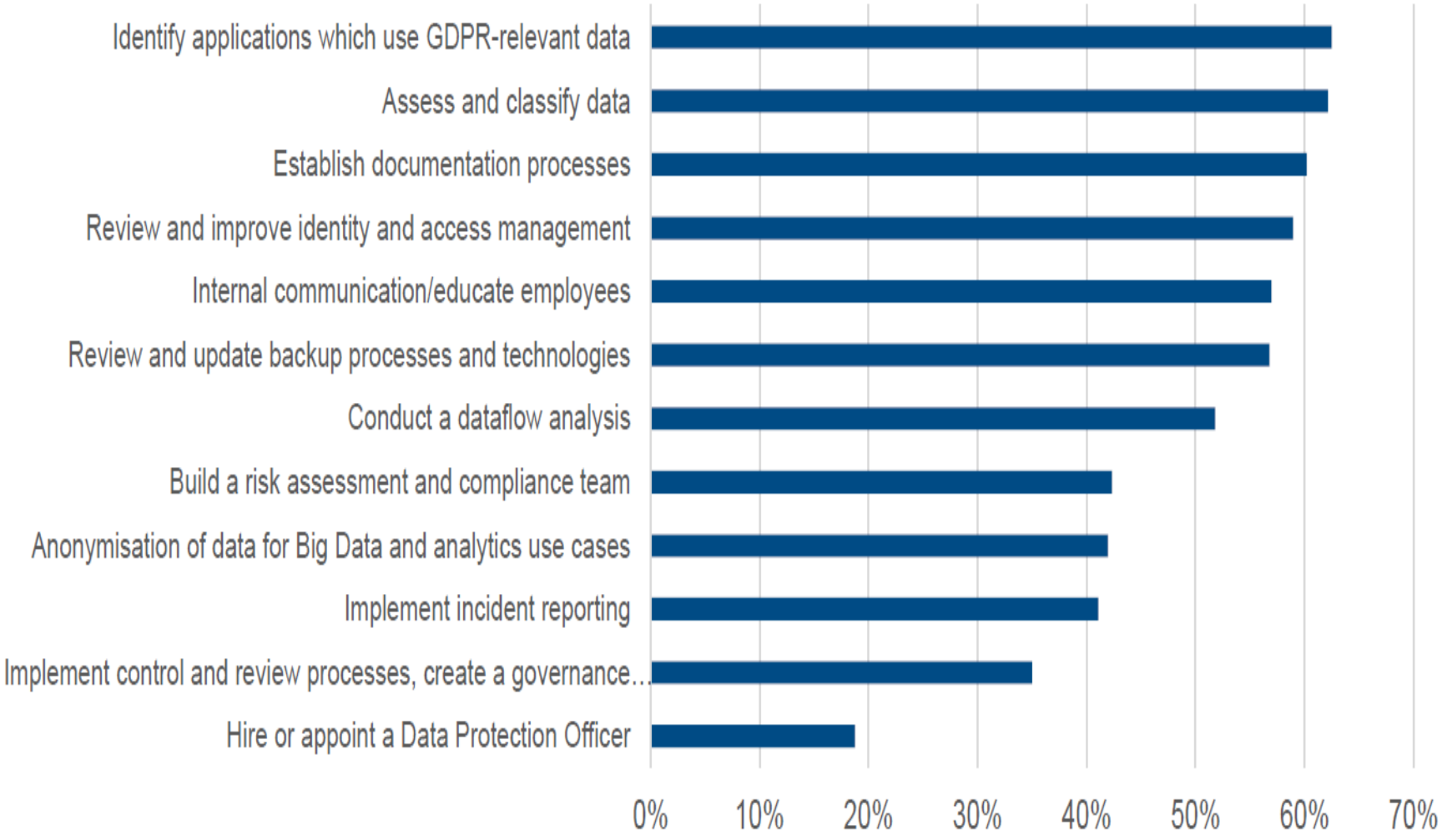
Fuente: IDC's 2017 GDPR survey, n=560

Situación de las organizaciones



Fuente: IDC's 2017 GDPR survey, n=560

Situación de las organizaciones



Fuente: IDC's 2017 GDPR survey, n=560

¿Reto u oportunidad?

Fuente: Liniers

Gracias por vuestra atención