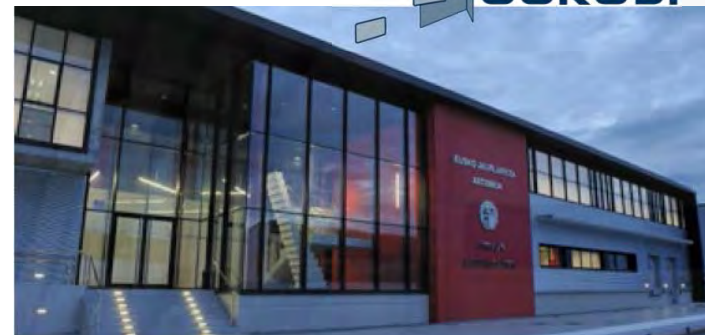




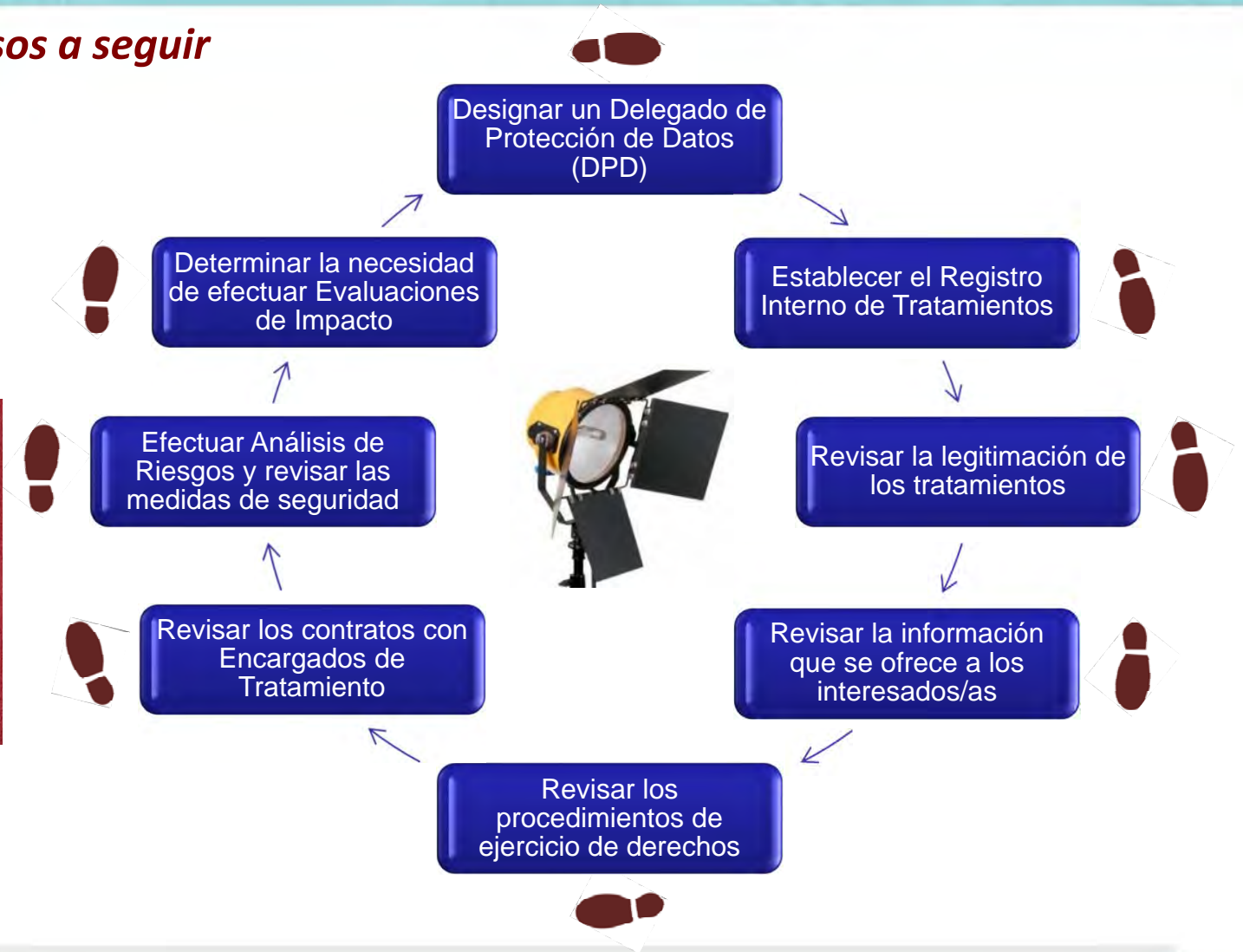
Implantación del nuevo Reglamento General de Protección de Datos en el Gobierno Vasco



Reflexiones sobre la adecuación al RGPD

Reflexiones sobre la adecuación al RGPD

Pasos a seguir



Reto del RGPD para la Gestión Documental



Transparencia

- Por diseño



Privacidad

- Por defecto y desde el diseño

1.456

PROCEDIMIENTOS
SERVICIOS

2.582

SERIES
DOCUMENTALES

6,1
millones

EXPEDIENTES
AKS/SGA

19,5
millones

DOCUMENTOS
ELECTRÓNICOS

61.000
metros lineales

DOCUMENTOS
PAPEL

2018: Datos de utilización de dokusi

Pasos a seguir



Establecer el Registro Interno de Tratamientos



El actual sistema de creación de Ficheros, mediante una disposición general, publicada en el BOPV y su notificación para la inscripción del mismo en la AVPD desaparece



REGISTRO DE
ACTIVIDADES DE
TRATAMIENTO

Se sustituye por el establecimiento de un Registro de actividades de tratamiento que es la pieza fundamental para demostrar el cumplimiento y facilitar la supervisión de los tratamientos

Ejie

El encargado de tratamiento también deberá llevar un registro interno de sus actividades



Como medida de transparencia, las AAPP harán público su registro de actividades de tratamiento, accesible por medios electrónicos. Deberá mantenerse actualizado y a disposición de las autoridades de protección de datos



Registro de actividades de tratamiento de la AEPD

Actividad de promoción	Gestión y control de la biblioteca
Agenda de la AEPD	Procedimientos de inspección de datos
Atención a los derechos de las personas	Provisión de puestos de trabajo
Consulta Previa Artículo 36 del RGPD	Quejas y sugerencias
Consultas	Recaudación
Encuestas y estudios	Régimen interior
Formación	Registro de Delegados de Protección de Datos
Gestión de autorizaciones y acreditaciones	Registro de E/S
Gestión de Brechas de Seguridad	Seguridad
Gestión de RRHH	Transparencia: acceso a la información
Gestión presupuestaria y económica	

Reflexiones sobre la adecuación al RGPD



Gestión de Brechas de Seguridad

a) Base jurídica	RGPD: 6.1.c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. Reglamento General de Protección de Datos. Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
b) Fines del tratamiento	Gestión y evaluación de las brechas de seguridad notificadas por los responsables de tratamiento.
c) Colectivo	Personas físicas, incluidas las representantes de personas jurídicas.
c) Categorías de Datos	Nombre y apellidos, dirección, firma y teléfono. Puesto en la entidad a la que representa.
d) Categoría destinatarios	Fuerzas y cuerpos de seguridad del Estado. Autoridades de control pertenecientes a la UE en el marco del desarrollo de las acciones conjuntas que se establecen el Título VII del RGPD. Equipos de respuesta ante emergencias informáticas (CERT) del Centro Criptológico Nacional y de los previstos en la Directiva 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
e) Transf. Internacional	No están previstas transferencias internacionales de los datos.
f) Plazo supresión	Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Será de aplicación lo dispuesto en la normativa de archivos y documentación.
g) Medidas de seguridad	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y que se encuentran descritas en los documentos que conforman la Política de protección de datos y seguridad de la información de la AEPD.
h) Entidad responsable	Agencia Española de Protección de Datos



Pasos a seguir



Revisar la legitimación de los tratamientos

En el caso de la actividad de las AAPP será muy habitual que la base jurídica de los tratamientos sea el cumplimiento de una **tarea en interés público** o el **ejercicio de poderes públicos**.

Tanto el interés público como los poderes públicos que justifican el tratamiento deben estar establecidos en una norma de rango legal



Las AAPP deberán identificar con precisión **las finalidades y la base jurídica de sus tratamientos**

En el caso de que el tratamiento esté basado en el consentimiento, habrá de tenerse en cuenta que **se han reforzado los requisitos para obtenerlo** («*informado, libre, específico y otorgado mediante una clara acción afirmativa*»), lo cual **invalida los consentimientos «tácitos**», es decir, basados en una inacción u omisión de acción por parte del interesado

Pasos a seguir para la adecuación al RGPD



Revisar la información que se ofrece a los interesados/as

Se ha reforzado la transparencia hacia el interesado/a, siendo la información a facilitar más amplia que la requerida hasta ahora



Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten