Pribatua

Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

Jornada VDE
Protección de datos, privacidad y ciberseguridad
Reglamento Europeo de Protección de Datos.

¿CÓMO AFECTA LA NUEVA NORMATIVA A LAS PYMES NAVARRAS?

¿QUÉ ES UN DPO/DPD Y QUÍEN LO NECESITA?

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

HOJA DE RUTA

- CONÓCETE A TI MISMO (aforismo griego)
- ¿Qué es nuestra organización?
  - Responsable de tratamiento
  - Encargado de tratamiento.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

CAMBIO ESENCIAL

- REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Desde la reflexión sobre el conocimiento de las actividades que se desarrollan se elabora el registro, como responsable de tratamiento y en su caso como encargado. (art. 30 RGPD).

Deberán estar a disposición de las autoridades de control.

(Desaparecida la obligación de inscribir registros)

(modelo AEPD)

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

DIFICULTADES

Identificar la legitimación del tratamiento.

- consentimiento
- relación contractual
- obligación legal
- proteger interés vital
- cumplimiento de una misión en interés público
- satisfacción de un interés legítimo (informe 2017/0159 AEPD)

Conocer y aplicar los plazos de conservación.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

TRANSPARENCIA EN EL TRATAMIENTO

- Derecho de transparencia.
  - Art. 13/14.
  - Derivado de la identificación de los registros de actividades permitirá cumplir con esta obligación.
  - Doble capa.

- Respuesta a pregunta en la jornada de la agencia: Las comunicaciones de datos a los encargados de tratamiento no se consideran cesiones de datos y no es necesario informar de ellas a los interesados.

TRANSPARENCIA EN EL TRATAMIENTO

- Consultas más frecuentes (FAQS)

- **4.4.- ¿Se debe cumplir con el contenido del derecho de información del RGPD para los tratamientos realizados antes de su aplicación?**
- Respecto a los afectados a quienes se les haya recabado sus datos de carácter personal con anterioridad a la aplicación del RGPD (25 de mayo de 2018), y que por tanto, se haya informado en los términos descritos por la LOPD, el responsable no tiene que enviar una comunicación al respecto con el contenido del derecho de información del RGPD. Es decir, este derecho de información del RGPD no se aplica de forma retroactiva. No obstante, desde la aplicación del RGPD todos los formularios o medios de recogida de datos personales, deberán adecuarse a la citada norma en aras de cumplir con el contenido del derecho de información que hemos descrito en las anteriores preguntas-respuestas.

ENCARGADOS DE TRATAMIENTO

ART. 28. Se elegirá únicamente al encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas.

Contrato

Pondrán a disposición del responsable información necesaria para acreditar el cumplimento.

ENCARGADOS DE TRATAMIENTO

4.6.- ¿Cómo se puede acreditar la existencia de garantías suficientes de un encargado de tratamiento?

Para demostrar que los encargados o subencargados ofrecen las garantías exigidas por el RGPD, éstos podrán adherirse a códigos de conducta o certificarse dentro de los esquemas previstos por el RGPD. Si bien antes el Reglamento de Desarrollo de la LOPD (RLOPD) establecía la necesidad de diligencia debida en la selección de encargados, según el RGPD el responsable deberá adoptar medidas apropiadas, incluida la elección de encargados, de forma que garantice y esté en condiciones de demostrar que el tratamiento se realiza conforme el RGPD (principio de responsabilidad activa).

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

ANALISIS DE RIESGOS

Es una obligación de todas las organizaciones.

- Las organizaciones han de ser “proactivas”, no han de esperan que las leyes les digan lo que hacer para proteger los derechos y libertades y en especial el derecho a la protección de datos.
- Al realizar el análisis de riesgos se identifican las medidas de seguridad que se deben aplicar.
- Obligaciones dirigidas a prevenir incumplimientos.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasunaren Euskal Elkartea

ANALISIS DE RIESGOS

- El análisis de riesgos se ha de realizar desde dos vertientes:
  - Desde la gestión de la seguridad de la información que tiene la organización.
    - ¿qué puede pasar en mi "casa"? Si tengo un incendio, se estropea el ordenador servidor y no tengo copias de seguridad.
  - Desde los derechos y libertades de las personas a las que les puede afectar nuestro tratamiento. Considerando 75
    - ¿cómo se ha de transmitir la información para que no sea accesible a terceros no autorizados?

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasunaren Euskal Elkartea

ANALISIS DE RIESGOS

- Es una herramienta esencial para el rendimiento de cuentas.
- Para demostrar que se han identificado los impactos que tendría la organización en caso de que se materialice la amenaza.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasunaren Euskal Elkartea

ANALISIS DE RIESGOS

- Fase Evaluación del Riesgo
- Clasificación de los estados posibles del Servicio.
- Identificación de los Activos.
- Identificación de las Amenazas.
- Relación de Amenazas Posibles sobre los Activos. Cálculo de la Probabilidad y Gravedad de las Amenazas.
- Valoración del Impacto.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasunaren Euskal Elkartea

ANALISIS DE RIESGOS

- Hemos analizado el riesgo inicial, teniendo en cuenta la gravedad y la probabilidad
- Identificado las vulnerabilidades,
- El impacto,

Y ahora toca definir las medidas ….

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasunako Euskal Elkartea

ANALISIS DE RIESGOS

- Fase Tratamiento del Riesgo
- Asumir el Riesgo
- Eliminar el Riesgo
- Transferir el Riesgo
- Tratar y Minimizar el Riesgo

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

EVALUACIÓN DE IMPACTO

- Cuando sea probable el tratamiento que entrañe un "alto riesgo", en particular si se utilizan nuevas tecnologías, antes del tratamiento se deberá efectuar una evaluación de impacto.
- En particular:
  - Evaluación sistemática y exhaustiva de aspectos personal, basado en tratamiento automatizado, elaboración de perfiles.
  - Tratamiento a gran escala de categorías especiales de datos, condenas e infracciones penales.
  - Observación sistemática a gran escala de una zona de acceso público.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

EVALUACIÓN DE IMPACTO

- Consultas más frecuentes (FAQS)

- **3.17.- Los tratamientos iniciados antes de la aplicación del RGPD ¿Deben someterse a una Evaluación de impacto?** No, el mandato del RGPD no se extiende a las operaciones de tratamiento que ya estén en curso en el momento en que comience a ser de aplicación. Sin embargo, sí debiera realizarse una Evaluación cuando en una operación iniciada con anterioridad a la aplicación del Reglamento se hayan producido cambios en los riesgos que el tratamiento implica en relación con el momento en que el tratamiento se puso en marcha. Este cambio en los riesgos puede derivar, por ejemplo, del hecho de que se hayan empezado a aplicar nuevas tecnologías a ese tratamiento, de que los datos se estén usando para finalidades distintas o adicionales a las que se decidieron en su momento, o de que se estén recogiendo más datos, o datos diferentes, de los que en principio se utilizaban para el tratamiento.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

BRECHAS DE SEGURIDAD

- RGPD define las "violaciones de seguridad de los datos personales" cuando se ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."
- No todos los incidentes de seguridad son brechas de seguridad de datos personales.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

BRECHAS DE SEGURIDAD

- Cuando el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales **debe** efectuar la correspondiente notificación a la autoridad de control competente, sin dilación y a más tardar en las 72 horas siguientes.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

BRECHAS DE SEGURIDAD

- La única excepción reside en si el responsable puede demostrar que la brecha de la seguridad de los datos personales no entraña un riesgo para los derechos y las libertades de las personas físicas.

BRECHAS DE SEGURIDAD

- Por el contrario, si supone un **alto riesgo** para los derechos y libertades de los titulares de los datos, además de la comunicación a la autoridad de control, el responsable del tratamiento deberá, adicionalmente, comunicar a los afectados la brecha de seguridad sin dilación y con lenguaje claro y sencillo.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

BRECHAS DE SEGURIDAD

- ¿Qué hacer?
- No se puede garantizar la seguridad al 100%, luego brechas de seguridad pueden aparecer y hay que estar preparado para saber gestionarlas.
- Procedimientos:
  - Clasificación.
  - Detección.
  - Respuesta a incidentes.
  - Notificación.

MEDIDAS DE SEGURIDAD

- Medidas de seguridad
  - Necesidad de acreditar el cumplimiento.

MEDIDAS DE SEGURIDAD

- PROTECCIÓN
  - Seguridad Física.
  - Seguridad Perimetral.
  - Sistemas Antivirus.
  - Actualización de los Sistemas.
  - Cifrado en los Dispositivos (portátiles, discos externos) para proteger la confidencialidad.
  - Copias de Seguridad (locales o en la nube) para proteger la disponibilidad.

MEDIDAS DE SEGURIDAD

- DETECCIÓN
  - Monitorización de los Sistemas.
  - Formación y Concienciación a los Trabajadores.
  - Auditorías de Seguridad.

MEDIDAS DE SEGURIDAD

- RESPUESTA ANTE INCIDENTES
  - Seguridad 100% no existe.
  - Restauraciones de las copias de seguridad realizadas.
  - Plan de Recuperación ante Desastres.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasunerako Euskal Elkartea

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

- En donde se da?
  - Tecnología informática, dispositivos, programas, aplicaciones ,....
  - Organización del tratamiento de los datos, de la propia organización que lo diseña y de terceros implicados.
  - Espacios físicos en los que se realiza el tratamiento.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información ikn
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

- Conexiones informáticas, interna, externas, utilización de alojamiento de información,....
- Modelo de gobierno de organización, procedimientos de trabajo....

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasunerako Euskal Elkartea

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

- La Doctora canadiense Ann Cavoukian,
  - Supera el planteamiento de la privacidad como un mero cumplimiento.
  - Devuelve al usuario el control sobre sus datos y a su divulgación.
  - El usuario tendrá más confianza en las empresas.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

- Los siete principios:
  - Proactivo no reactivo; Preventivo no remediar, valorar la privacidad antes no después.
  - Privacidad como valor predeterminado.
  - Privacidad incrustada, entretejida, en el diseño.
  - Funcionalidad completa - suma positiva, no suma cero, responde a la necesidad de la empresa.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

- Seguridad de extremo a extremo: protección completa del ciclo de vida.
- Visibilidad y transparencia - manténgalo abierto.
- Respeto a la privacidad del usuario - mantenerlo centrado en el usuario, todo gira entorno al usuario

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

- Se ha producido, por primera vez, la extensión de la metodología del diseño a una norma legal.
- Es la revisión del contexto desde el planteamiento integral y transversal en el que nada se debe dar por sentado.

Pribatua

DELEGADO DE PROTECCIÓN DE DATOS

- Art. 37 RGPD Obligatorio en :
  - Sector público
  - Actividades principales que requieran una observación habitual y sistemática de interesados a "gran escala". (Considerando 91)
  - Actividades principales que consistan en tratamiento a "gran escala" de categorías especiales de datos (art. 9) y datos relativos a condenas e infracciones penales

ART.34 proyecto de ley.

DELEGADO DE PROTECCIÓN DE DATOS

- Requisitos / cualidades profesionales del DPD.
  - Se designa atendiendo a:
    - sus cualidades profesionales,
      - en especial conocimiento especializados en derecho y práctica en materia de protección de datos,
    - Capacidad para desempeñar las funciones designadas en el artículo 39.

Pribatua

DELEGADO DE PROTECCIÓN DE DATOS

- **Habilidades y experiencia:**
- Experiencia en las leyes y practicas nacionales y europeas en materia de protección de datos, incluida una comprensión en profundidad del RGPD
- Comprensión de las operaciones de tratamiento realizadas
- Comprensión de las tecnologías de la información y la seguridad de los datos

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Arbitratuen eta Informazio Segurtasunerako Euskal Elkartea

DELEGADO DE PROTECCIÓN DE DATOS

Habilidades y experiencia:

- Conocimiento del sector empresarial y de la organización
- Capacidad para promover una cultura de protección de datos.
- Acreditar cualidades profesionales.
  - Titulación
  - Acreditación
- El mecanismo de certificación de ENAC

DELEGADO DE PROTECCIÓN DE DATOS

- ¿Quién puede ser DPD?

El DPD puede ser un miembro del personal del responsable del tratamiento o del encargado del tratamiento (**DPD interno**) o «cumplir las tareas sobre la base de un **contrato de servicios**». Puede ejercerse sobre la base de un contrato de servicios celebrado con un individuo u organización

- Equipo de personas bajo la responsabilidad del contrato designado
- Cada miembro del equipo debe cumplir los requisitos del RGPD

Pribatua

DELEGADO DE PROTECCIÓN DE DATOS

- Funciones:
  - Informar y asesorar al responsable.
  - Supervisar el cumplimiento de lo dispuesto en el RGPD.
  - Supervisar la realización de la evaluación de impacto.
  - Cooperar con la autoridad de control.
  - Supervisar la gestión de quiebras de seguridad.
  - Cooperar como Punto de contacto con la autoridad de control.
  - Información directa a la dirección.

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Euskadiko Pribatutasun eta Informazio Segurtasunaren Elkartea / Euskera

DELEGADO DE PROTECCIÓN DE DATOS

Salvaguardas

- Ninguna instrucción de los controladores lo procesadores sobre el ejercicio de las tareas del DPD
- Ningún despido o sanción por parte del controlador para el desempeño de las tareas del DPD
- •No hay conflicto de intereses con otras posibles tareas y deberes

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

DELEGADO DE PROTECCIÓN DE DATOS

- ¿Es obligatorio en nuestra organización?

- Directriz sobre delegado de protección de datos del grupo de trabajo del artículo 29. (actualmente ya se ha constituido el Comité).
  - Actividad principal.
  - Gran escala

SANCIONES

ART. 83 RGPD.

SANCIONES ADMINISTRATIVAS DE :

10.000.000.- € / 2% del volumen de negocio total anual
20.000.000.- € / 4% del volumen de negocio total anual

Pribatua

Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

VERIFICACIÓN DE CUMPLIMIENTO (I)

REGISTRO DE ACTIVIDADES, (responsable de tratamiento o encargado de tratamiento).

INFORMACIÓN A LOS INTERESADOS (impresos de recogida de datos, formularios on line).

REVISAR SI CUMPLIMOS CON LOS PRINCIPIOS DEL REGLAMENTO.

IDENTIFICACIÓN DE LA BASE DE LEGITIMACIÓN.

MEDIOS EJERCICIO INTERESADOS

CONTRATOS CON ENCARGADOS DE TRATAMIENTO.

VERIFICACIÓN DE CUMPLIMIENTO (II)

MEDIDAS DE RESPONSABILIDAD PROACTIVA:

- análisis de riesgos.
- privacidad desde el diseño y por defecto
- cifrado de la información

PROCEDIMIENTO PARA QUIEBRAS DE SEGURIDAD

NOMBRAMIENTO DELEGADO DE PROTECCIÓN DE DATOS

Pribatua
Asociación Vasca de Privacidad y Seguridad de la Información
Pribatutasun eta Informazio Segurtasuneko Euskal Elkartea

GRACIAS