BROSETA
+50 años

Criterios administrativos sancionadores y jurisprudenciales relativos a los incidentes de seguridad en materia de protección de datos personales

Julio 2025

ÍNDICE

1 TENDENCIAS DE LAS AUTORIDADES DE CONTROL

España

Data breach: evolución de la Agencia Española de Protección de Datos (**AEPD**).

Más de 100 infracciones consecuencia de la concurrencia de brechas de seguridad.

En 2024 la AEPD ha impuesto multas por 12,8M€ (47'5% del total).

Sectores más afectados: *retail*, energía, banca y telecomunicaciones.

Italia

79.1M€ - Sanción a suministrador eléctrico

Irlanda

265M€ - Sanción a red social

Reino Unido

20.4M€ - Sanción a cadena hotelera

En España: mucha actividad sancionadora, con importes de multas "menores".

En Europa: menor actividad de las autoridades de control, pero importes mayores.

2 TIPOS DE BRECHAS DE SEGURIDAD

Disponibilidad

Datos inaccesibles temporal o permanentemente

Confidencialidad

Acceso no autorizado a datos

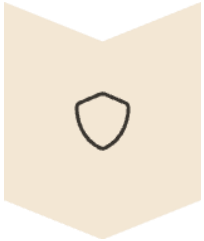
Integridad

Alteración ilegítima de datos

Ausencia de **notificación** o **notificación tardía** de la brecha a la autoridad de control y/o interesados

Incumplimiento del principio de ***Privacy by Design*** o ***by Default***

3 ACTUACIÓN ANTE UNA BRECHA DE SEGURIDAD



Contención inmediata

Medidas reactivas para detener la brecha

Análisis de severidad

Evaluar el impacto y riesgo

Notificación AEPD

En 72 horas si hay riesgo alto

Comunicación afectados

Si existe alto riesgo para sus derechos

4 PROCEDIMIENTO ANTE LA AEPD

Notificación

Comunicación a la AEPD dentro de 72 horas desde la detección

Investigación (18 meses)

La División de Innovación Tecnológica de la AEPD analiza el caso

Puede requerir información adicional al Responsable del tratamiento

Si procede, la AEPD abre procedimiento sancionador

Procedimiento Sancionador (12 meses)

Contencioso Administrativo

Posibilidad de recurrir las decisiones de la AEPD ante la Audiencia Nacional

5 RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

Responsable de tratamiento

- El Responsable del tratamiento responde tanto por el tratamiento de datos personales que lleve a cabo directamente como por los realizados en su nombre (salvo supuestos excepcionales).
- Motivo de la exigencia de responsabilidad: obligación de seleccionar un Encargado que garantice el cumplimiento de la norma (*culpa in eligendo*) y supervisar su actuación (*culpa in vigilando*).

Encargado del tratamiento

- El Encargado únicamente tratará los datos personales siguiendo las instrucciones del Responsable, sin decidir sobre los fines y medios de dicho tratamiento
- Si la brecha se produce en los sistemas del Encargado del tratamiento, este debe informar inmediatamente acerca de su existencia al Responsable
- En general, sólo responde en caso de haber destinado los datos personales a sus propios fines, excediendo los límites del encargo, al tener en ese caso la condición de responsable

6 PRINCIPALES INFRACCIONES

Art. 5.1.f RGPD

Pérdida de confidencialidad o integridad (obligación de resultado)

Art. 32 RGPD

Insuficiencia de medidas técnicas y organizativas (obligación de medios)

Art. 25 RGPD

Falta de protección desde el diseño y por defecto

Art. 33 y 34 RGPD

No notificar a la AEPD/interesados en plazo y forma

El RGPD distingue dos tipos de infracciones a efectos de la sanción aplicable:

- Las infracciones que pueden sancionarse con hasta 20 millones de euros o el 4 % del volumen de negocio anual global (art. 5.1.f RGPD)
- Las infracciones que pueden sancionarse con hasta 10 millones de euros o el 2 % del volumen de negocio anual global (arts. 25, 32, 33 y 34 RGPD)

Art. 5.1.f RGPD

Pérdida de confidencialidad, disponibilidad o integridad

- Se trata de una obligación de resultado "***garantizar*** *una* ***seguridad adecuada****, incluida la protección contra el tratamiento no autorizado o ilícito u contra su pérdida, destrucción o daños accidental, mediante la aplicación de medidas* ***técnicas*** *y* ***organizativas apropiadas***"
- Se trata no solo de medidas técnicas, sino también organizativas.
- Necesidad de evaluar exhaustivamente los riesgos asociados al tratamiento de datos, considerando su probabilidad y gravedad en relación a los derechos y libertades de los interesados.
- No es necesario se produzca un daño "tangible" para considerar cometida la infracción, bastando que se produzca una exposición o tratamiento no autorizado (confidencialidad) o pérdida de control por el interesado (disponibilidad)

Art. 32.RGPD

Insuficiencia de medidas de seguridad

- Se trata de una obligación de medios (STS 15/02/22).
- Debe evaluarse la diligencia en la implementación de las medidas, previa la evaluación del riesgo que deben estar efectivamente implementadas.
- Obligación dinámica: en el momento inicial del tratamiento y durante el mismo.
- Deben focalizarse en los riesgos para los derechos y libertades de los interesados, no en los riesgos de seguridad que impacten únicamente en la organización: de este modo, los estándares (e.g: ISO 27001) no garantizan el cumplimiento de esta obligación, aunque lo faciliten.

Art. 25.RGPD

Falta de protección desde el diseño y por defecto

- Necesidad de aplicar, en el momento de determinar los medios del tratamiento, como durante el mismo, medidas diseñadas para garantizar la aplicación efectiva de los principios de protección de datos.
- No se trata únicamente del principio de integridad y confidencialidad, sino cualquier otro (e.g: principio de minimización, finalidad…)
- Enfoque de las medidas orientado a los riesgos sobre los derechos y libertades, no sobre riesgos legales o tecnológicos (aunque estén relacionados).
- Necesidad por el responsable de actitud proactiva, actuando de forma sistemática, preventiva y global, con una estrategia orientada al cumplimento RGPD.

Art. 33 y 34 RGPD

Notificación a la AEPD y a los afectados

- No es necesario se materialice el riesgo, basta con que exista la posibilidad de que el riesgo ocurra.
- La simple pérdida de confidencialidad, constituye “per se” un riesgo probable.
- No será necesaria la comunicación si es improbable que la brecha suponga un riesgo (e.g: datos encriptados).
- La demora en cumplimentar los plazos deberá justificarse.
- Comunicación a los interesados: accesible, comprensible y con instrucciones claras sobre como proceder si los datos están comprometidos.

7 CULPABILIDAD Y RESPONSABILIDAD

Consideraciones relevantes

1.- Concurrencia de las infracciones 5.1f) y 32 del RGPD: *non bis idem* y concurso medial.

- Inicialmente: infracciones autónomas e independientes (situaciones donde las medidas técnicas organizativas son inadecuadas sin producirse perdida de datos ***vs*** situaciones con medidas de seguridad técnicamente adecuadas que no evitan la brecha).
- Evolución hasta apreciar la concurrencia de un concurso medial: aunque el ámbito del artículo 5 no se circunscribe a la obligación de medidas de seguridad, si la confidencialidad se ha visto comprometida como consecuencia de la insuficiencia de las medidas de seguridad (se sanciona ex art.5 y no art.32 porque no se observa conculcación de otras medidas de seguridad u organizativas independientes o distintas de las relacionadas con la brecha)

2.- Culpabilidad y responsabilidad: no es posible la responsabilidad objetiva (mera producción del resultado)

- El elemento culpabilístico se traduce en la ausencia de la diligencia debida- negligencia al no implementar las medidas adecuadas conforme a los riesgos considerando naturaleza, alcance, contexto y fines del tratamiento.

8 AGRAVANTES Y ATENUANTES

Circunstancias agravantes

- Naturaleza, gravedad y duración de la infracción: "*la gravedad de la infracción es consustancial al hecho típico que se sanciona*" (SAN 8/05/25)
- Intencionalidad o negligencia del responsable: "*es el elemento subjetivo consustancial al hecho típico… debe acreditarse un plus de intencionalidad*" (SAN 8/05/25)
- Vinculación del infractor con la realización de datos personales + gran empresa + carácter continuado + número de interesados afectados + perjuicios causados.

Circunstancias atenuantes

No suelen apreciarse algunas como: grado cooperación con AEPD; medidas para mitigar perjuicios, ausencia beneficio económico o coste asumido para mitigar daños e implementación de medidas que eviten su producción futura.

Madrid. Paseo de la Habana, 101. 28036. T. +34 91 432 31 44
Barcelona. Tuset, 23. 08006. T. +34 93 362 05 45
Valencia. Pascual y Genís, 5. 46002. T. +34 96 392 10 06
Lisboa. Av. António Augusto de Aguiar, 15. 1050-012. T. +351 300 509 035
Zúrich. Schifflände 22. 8001. T. +41 445 51 45 22
info@broseta.com · **www.broseta.com**

España · Portugal · Suiza · Red Legal Iberoamericana