Agosto 2023
Notificaciones de Brechas de Datos Personales

Agencia Española de Protección de Datos
División de Innovación Tecnológica
Septiembre 2023

1. DESTACADO

En muchos casos, en un tratamiento de datos personales participan múltiples organizaciones con distintos tipos de roles en relación con la protección de datos. Estos escenarios incluyen casos de cesiones de datos entre responsables y responsable-encargado.

En estos casos, puede concentrarse un volumen muy elevado de datos en infraestructuras tecnológicas, a veces en la nube, a los que tienen acceso múltiples entidades. Estas infraestructuras son especialmente atractivas para los ciberdelincuentes, y aún más cuando los datos tratados son de categorías especiales, como podrían ser datos de salud en el ámbito sanitario.

Cuando ocurre un incidente de seguridad que afecte a datos personales en esa infraestructura, a menudo se observan deficiencias en la respuesta y la gestión de la brecha por las discrepancias en cuanto al rol responsable/encargado de cada una de las entidades que participan en el tratamiento. Que en un tratamiento las entidades no tengan claro su rol de responsable/encargado es ya un incumplimiento del RGPD, al evidenciar que no se está cumpliendo con obligaciones básicas como las establecidas en el art.28 del RGPD respecto a las obligaciones de responsables y encargados, el art.25 sobre la aplicación de la protección de datos desde el diseño.

Además, si es necesario comunicar la brecha a los interesados afectados conforme al art. 34 del RGPD pero surgen discrepancias sobre qué entidad es el responsable del tratamiento y debe llevarla a cabo, se producirán retrasos en la comunicación o ésta no llega a producirse, incumpliendo el mismo art. 34, pero también el principio de responsabilidad proactiva establecido en el art.5.2 del RGPD.

En todo tratamiento de datos personales, pero especialmente en tratamientos complejos en los que participan múltiples entidades, los roles de responsable/encargado deben estar perfectamente definidos desde el diseño para cada tratamiento, se deben establecer medidas técnicas y organizativas adecuadas al nivel de riesgo, se deben prever situaciones de brechas de datos personales y establecer procedimientos adecuados para una rápida respuesta y gestión ante una eventual brecha.

Una EIPD previa conforme al art. 35 del RGPD, permite analizar la necesidad y proporcionalidad del tratamiento y permite evaluar el supuesto beneficio de tratamiento frente al riesgo de las posibles consecuencias negativas de una brecha de datos personales.

- 111 notificaciones recibidas, 106 de ellas a través del formulario en Sede Electrónica[1].
- 29 son notificaciones con información adicional.
- 85 notificaciones por parte de organizaciones del ámbito privado.
- 87 notificaciones indican brecha de confidencialidad, 2 de integridad y 39 de disponibilidad (algunas brechas presentan más de una tipología).
- 80 notificaciones indican origen externo.
- 72 notificaciones indican carácter malintencionado.

[1] Las siguientes cifras se refieren exclusivamente a las notificaciones recibidas mediante el formulario de notificación de brechas de datos personales en Sede Electrónica.

- 26 notificaciones de brechas implican categorías especiales de datos, de las cuales 24 se refieren a datos de salud.
- 73 notificaciones indican severidad de las consecuencias para los afectados baja.
- 0 notificaciones indican severidad muy alta.
- 19 notificaciones de brechas con implicaciones de carácter transfronterizo.
- La notificación de brecha con mayor número de afectados indica aproximadamente 1600000 personas afectadas.
- 35 notificaciones indican haber comunicado la brecha en total a aproximadamente 50276 personas.
- 21 notificaciones indican que comunicarán la brecha en total a aproximadamente 1621479 afectados.
- 28 notificaciones indican que no informarán a los afectados.

2. DETALLE DE NOTIFICACIONES

En este informe se resumen las características principales de las notificaciones de brechas de datos personales recibidas en la Agencia Española de Protección de Datos (AEPD) en virtud del artículo 33 del Reglamento (UE) 2016/679, General de Protección de Datos.

El informe recoge las notificaciones de brechas de datos personales recibidas durante agosto de 2023, siendo un total de 111 notificaciones, de las cuales 106 han utilizado como canal de comunicación el formulario de "notificación de brechas de datos personales" publicado en la sede electrónica.

Los datos indicados en este apartado corresponden al contenido de las notificaciones de datos personales recibidas exclusivamente a través del formulario en Sede Electrónica.

Entrada de notificaciones:

Descripción	Total
Notificaciones recibidas	111
Formulario sede electrónica	106
Otros medios	5

Evolución notificaciones[2]:

	Total
Total 2021	**1647**
Total 2022	**1751**
Acumulado últimos 12 meses	**2035**
ago-22	181
sep-22	189
oct-22	166
nov-22	209
dic-22	170
ene-23	142
feb-23	149
mar-23	208
abr-23	214
may-23	158
jun-23	184
jul-23	135
ago-23	**111**

Tipo de notificación:

Tipo	Total
Nueva	77
Inicial	40
Completa	37
Modificación	29

[2] Estas cifras se refieren al total de notificaciones recibidas por cualquier canal de comunicación.

Tipo de organización:

Descripción	Total
Organizaciones privadas	85
Organizaciones públicas	21

Tipología de la brecha de datos personales:

Tipo	Total
Confidencialidad	87
Integridad	2
Disponibilidad	39

Tratamiento de las brechas de datos personales:

Descripción	Total
Resueltas	60
No resueltas o no indicado	46

Medios de materialización de las brechas de datos personales:

Medios	Total
Revelación verbal no autorizada	2
Documentación perdida, robada	11
Correo postal perdido, abierto	2
Eliminación incorrecta de datos en formato papel	0
Datos enviados por error (postal o electrónicamente)	11
Datos personales eliminados / destruidos	0
Abuso de privilegios de acceso	2
Datos residuales en dispositivos obsoletos	0
Publicación no intencionada / autorizada	5
Envío de correo electrónico a múltiples destinatarios sin cco	4
Dispositivo perdido o robado	2
Ciberincidente: Dispositivo cifrado / secuestro de información	46
Ciberincidente: Suplantación de identidad (phishing)	19
Ciberincidente: Acceso no autorizado a datos en SI	32
Incidencia técnica	2
Modificación no autorizada de datos	1
Datos personales mostrados al individuo incorrecto	7

Contexto de la brecha de datos personales:

Origen / Intencionalidad	Total
Interno Responsable	19
Interno Encargado	7
Externo	80
Accidental	26
Malintencionado	72
Intencionalidad desconocida	8

Categorías de datos:

Categorías	Total
Categorías Especiales	26
Condenas e inf. penales	3

Detalle categorías especiales:

Medios	Total
Sobre la religión o creencia	2
Sobre el origen racial	4
Sobre la opinión política	0
De salud	24
Sobre la afiliación sindical	2
Sobre la vida sexual	0
Genéticos	3
Biométricos	2

Perfiles de los afectados:

Afectados	Total
Clientes / Ciudadanos	72
Estudiantes / Alumnos	4
Usuarios	16
Pacientes	11
Suscriptores / Clientes potenciales	10
Afiliados / Asociados	1
Militares / Policía	0
Empleados	50
Otros	20

Severidad de las consecuencias para los interesados:

Severidad	Total
Baja	73
Media	10
Alta	5
Muy alta	0
Desconocida	18

Número de afectados:

Afectados	Total
[0-99]	37
[100-999]	36
[1000-9999]	30
[10000-99999]	2
[100000-999999]	0
[1000000-99999999]	1

Evolución comunicaciones a los interesados :

	Han sido informados[3] o Serán informados[4] (cifra aproximada)
Total 2021	**12.996.000**
Total 2022	**30.828.000**
Acumulado últimos 12 meses	**17.516.000**
ago-22	2.434.000
sep-22	375.000
oct-22	4.466.000
nov-22	2.668.000
dic-22	2.371.000
ene-23	141.000
feb-23	256.000
mar-23	1.390.000
abr-23	3.029.000
may-23	312.000
jun-23	181.000
jul-23	656.000
ago-23	**1.671.000**

[3] En la notificación de brecha de datos personales se indica que los interesados han sido informados.
[4] En la notificación de brecha de datos personales se indica que los interesados serán informados.

Notificaciones por Comunidades Autónomas:

Comunidad Autónoma	Total
Andalucía	13
Aragón	0
Principado de Asturias	0
Baleares	1
Cantabria	3
Castilla y León	9
Castilla-La Mancha	3
Cataluña	19
Comunidad Valenciana	6
Extremadura	1
Galicia	6
Comunidad de Madrid	33
Región de Murcia	2
Comunidad Foral de Navarra	2
País Vasco	1
La Rioja	0
Canarias	2
Ceuta	0
Melilla	0

Implicaciones transfronterizas:

Notificaciones con afectados en otros Estados Miembro: 19

Estado	Total
ALEMANIA	12
AUSTRIA	6
BELGICA	9
BULGARIA	1
REPÚBLICA CHECA	2
CHIPRE	1
CROACIA	2
DINAMARCA	4
FRANCIA	16
ESLOVAQUIA	1
ESLOVENIA	1
ESTONIA	1
FINLANDIA	4

Estado	Total
GRECIA	5
HUNGRIA	2
IRLANDA	6
ITALIA	8
LETONIA	0
LITUANIA	1
LUXEMBURGO	2
MALTA	2
PAISES BAJOS	6
PORTUGAL	9
RUMANIA	1
SUECIA	4
POLONIA	4