Junio 2026
Notificaciones de Brechas de Datos Personales

Agencia Española de Protección de Datos
División de Innovación Tecnológica
Julio 2026

1. DESTACADO

La identificación no exige conocer el nombre civil de la persona. Basta con que los datos permitan distinguirla de las demás, seguirla en el tiempo, vincular información a un mismo individuo o reidentificarla mediante información adicional razonablemente disponible. Por ello, los datos sin nombre, DNI, teléfono o correo electrónico pueden seguir siendo datos personales si contienen identificadores seudónimos, identificadores en línea, patrones únicos o combinaciones de atributos que hagan identificable o singularizable a la persona.

Esto es debido a que la definición de dato personal conforme al art. 4.1 del RGPD es muy amplia al incluir los datos de personas físicas “identificables”.

Una persona es identificable si su identidad puede determinarse, directa o indirectamente, por cualquier medio, incluyendo el uso de identificadores como números de identificación, datos de localización, identificadores en línea o factores específicos de su identidad física, fisiológica, genética, psíquica, económica, cultural o social. Ejemplo: Un número de cliente en una base de datos interna puede ser un dato personal si puede vincularse a un individuo concreto.

El Dictamen 4/2007 del grupo de trabajo del artículo 29 (WP29) sobre el concepto de dato personal sentó las bases para entender que los datos personales no se limitan a los identificadores directos (nombre, apellidos, DNI, etc.), sino que incluyen cualquier información que permita singularizar a una persona física, incluso de forma indirecta (incluso si requiere el cruce con otros datos o el uso de claves de reidentificación).

El WP29 introduce el concepto de "singularización" (singling out), que se refiere a la capacidad de aislar a un individuo dentro de un grupo mediante la combinación de datos. Incluso si no se conoce su nombre, si es posible distinguirlo de los demás, el dato es personal.

Ejemplo: En un conjunto de datos sin identificadores directos sobre hábitos de compra, si un registro permite identificar a una persona como "el único cliente que compró el producto X en la tienda Y el día Z", ese registro es un dato personal.

Para entenderlo y aplicarlo correctamente, es importante tener en cuenta la diferencia entre pseudonimización y anonimización.

En el caso de la pseudonimización los datos se procesan de manera que ya no pueden atribuirse a un sujeto sin información adicional (ej.: hashes, tokens, números de cliente, etc). Sin embargo, siguen siendo datos personales, porque la reidentificación es posible si se accede a esa información adicional.

Ejemplo: Un hospital que asigna un código único a cada paciente en lugar de usar su nombre. Si el hospital conserva la clave para vincular el código a la identidad paciente, los datos son personales. Incluso cuando no conserve esas claves, si es posible identificar a los pacientes de cualquier otra forma, los datos seguirán siendo personales.

La pseudonimización es una herramienta de protección de datos desde el diseño que reduce el riesgo, pero no elimina el carácter personal de los datos.

En el caso de la anonimización los datos se modifican de forma irreversible, de modo que no existe ninguna posibilidad (ni siquiera para el responsable del tratamiento) de reidentificar al individuo.

- 185 son notificaciones con información adicional.
- 375 notificaciones por parte de organizaciones del ámbito privado.
- 418 notificaciones indican brecha de confidencialidad, 20 de integridad y 108 de disponibilidad (algunas brechas presentan más de una tipología).
- 338 notificaciones indican origen externo.
- 339 notificaciones indican carácter malintencionado.
- 68 notificaciones de brechas implican categorías especiales de datos, de las cuales 63 se refieren a datos de salud.
- 324 notificaciones indican severidad de las consecuencias para los afectados baja.
- 4 notificaciones indican severidad muy alta.
- 81 notificaciones de brechas con implicaciones de carácter transfronterizo.

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 junio de 2026, siendo un total de 518 notificaciones, de las cuales 477 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	518
Formulario sede electrónica	**477**
Otros medios	41

Evolución notificaciones[1]:

	Total
Total 2024	**2933**
Total 2025	**2765**
Acumulado últimos 12 meses	**4494**
jun-25	227
jul-25	282
ago-25	176
sep-25	235
oct-25	287
nov-25	216
dic-25	268
ene-26	216
feb-26	287
mar-26	786
abr-26	527
may-26	696
jun-26	**518**

Tipo de notificación:

Tipo	Total
Nueva	292
Inicial	149
Completa	143
Modificación	185

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

Tipo de organización:

Descripción	Total
Organizaciones privadas	375
Organizaciones públicas	102

Tipología de la brecha de datos personales:

Tipo	Total
Confidencialidad	418
Integridad	20
Disponibilidad	108

Tratamiento de las brechas de datos personales:

Descripción	Total
Resueltas	333
No resueltas o no indicado	144

Medios de materialización de las brechas de datos personales:

Medios	Total
Revelación verbal no autorizada	4
Documentación perdida, robada	14
Correo postal perdido, abierto	14
Eliminación incorrecta de datos en formato papel	0
Datos enviados por error (postal o electrónicamente)	52
Datos personales eliminados / destruidos	2
Abuso de privilegios de acceso	16
Datos residuales en dispositivos obsoletos	2
Publicación no intencionada / autorizada	23
Envío de correo electrónico a múltiples destinatarios sin cco	14
Dispositivo perdido o robado	25
Ciberincidente: Dispositivo cifrado / secuestro de información	123
Ciberincidente: Suplantación de identidad (phishing)	133
Ciberincidente: Acceso no autorizado a datos en sistema de información	201
Incidencia técnica	18
Modificación no autorizada de datos	7
Datos personales mostrados al individuo incorrecto	30

Contexto de la brecha de datos personales:

Origen / Intencionalidad	Total
Interno responsable	102
Interno encargado	37
Externo	338
Accidental	124
Malintencionado	339
Intencionalidad desconocida	14

Categorías de datos:

Categorías	Total
Categorías Especiales	68
Condenas e inf. penales	7

Detalle categorías especiales:

Medios	Total
Sobre la religión o creencia	4
Sobre el origen racial	3
Sobre la opinión política	1
De salud	63
Sobre la afiliación sindical	3
Sobre la vida sexual	1
Genéticos	0
Biométricos	1

Perfiles de los afectados:

Afectados	Total
Clientes / Ciudadanos	315
Estudiantes / Alumnos	57
Usuarios	75
Pacientes	21
Suscriptores / Clientes potenciales	13
Afiliados / Asociados	10
Militares / Policía	1
Empleados	185
Otros	61

Severidad de las consecuencias para los interesados:

Severidad	Total
Baja	324
Media	77
Alta	20
Muy alta	4
Desconocida	52

Número de afectados:

Afectados	Total
[0-99]	193
[100-999]	148
[1000-9999]	94
[10000-99999]	30
[100000-999999]	8
[1000000-99999999]	4
[10000000-99999999]	0
Otro	0

Evolución comunicaciones a los interesados:

	Han sido informados[2] o Serán informados[3] (cifra aproximada)
Total 2024	**96.601.000**
Total 2025	**209.281.000**
Acumulado últimos 12 meses	**225.350.000**
jun-25	2.286.000
jul-25	9.489.000
ago-25	413.000
sep-25	911.000
oct-25	57.713.000
nov-25	60.129.000
dic-25	24.914.000
ene-26	10.328.000
feb-2026	21.976.000
mar-2026	7.238.000
abr-26	12.263.000
may-26	2.696.000
jun-26	**17.280.000**

Notificaciones por Comunidades Autónomas:

Comunidad Autónoma	Total
Andalucía	48
Aragón	15
Principado de Asturias	7
Baleares	14
Cantabria	3
Castilla y León	11
Castilla-La Mancha	9
Cataluña	76
Comunidad Valenciana	50
Extremadura	7
Galicia	18
Comunidad de Madrid	147
Región de Murcia	22
Comunidad Foral de Navarra	17
País Vasco	6
La Rioja	5
Canarias	15
Ceuta	1
Melilla	2

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

Implicaciones transfronterizas:

Notificaciones con afectados en otros Estados Miembro: 81

Estado	Total
ALEMANIA	59
AUSTRIA	24
BELGICA	37
BULGARIA	12
REPÚBLICA CHECA	19
CHIPRE	8
CROACIA	13
DINAMARCA	17
FRANCIA	59
ESLOVAQUIA	14
ESLOVENIA	15
ESTONIA	14
FINLANDIA	11

Estado	Total
GRECIA	13
HUNGRIA	19
IRLANDA	33
ITALIA	47
LETONIA	8
LITUANIA	12
LUXEMBURGO	19
MALTA	7
PAISES BAJOS	45
PORTUGAL	44
RUMANIA	23
SUECIA	24
POLONIA	29