

## Ante una brecha de datos personales, ¿cuándo y cómo se debe comunicar a los afectados? (art. 34 RGPD)



### ¿Para qué?

Proteger a las personas ante las consecuencias de una brecha de datos personales.

### ¿Cuándo?

Cuando se produzca un riesgo alto para derechos y libertades de las personas.

### ¿A quién?

A aquellas personas físicas que se encuentren en alto riesgo debido a la brecha.

### ¿Plazo?

**Sin dilación indebida.**  
Antes de que las consecuencias puedan afectar a las personas y con tiempo para que se protejan.

### ¿Cómo?

**Con una comunicación dirigida a cada uno de los afectados.**

Por ejemplo, mediante email, SMS, mensajería instantánea o correo postal.

Si supone un esfuerzo desproporcionado o se desconoce con precisión quién ha podido verse afectado, se puede realizar un comunicado público que tenga la misma eficacia.

## Contenido mínimo de la comunicación



### Naturaleza

#### Qué ha ocurrido.

Describir si se trata de un ciberincidente, ciberataque, envío de datos por error, pérdida de documentación/dispositivo, etc.

#### A qué datos ha afectado.

Especificar si concierne a datos básicos, de contacto, email, usuario y contraseña, copias de DNI o pasaporte, contratos, facturas, perfiles, localizaciones, etc.

#### De qué manera.

Concretar si es por un acceso ilegítimo, datos extraídos, revelados a terceros o públicos, alterados, eliminados, inservibles o no disponibles, etc.

### Consecuencias

#### Qué impacto puede tener sobre las personas.

Menoscabo en sus derechos fundamentales, imposibilidad de ejercer otros derechos, suplantación de identidad, imposibilidad de prestar correctamente un servicio, fraude, discriminación, daños físicos o psicológicos, entre otras.

#### Circunstancias agravantes.

El destinatario de sus datos es la persona denunciada por usted, la contraseña comprometida se usa en otros servicios, los datos se han publicado de forma abierta en internet, etc.

### Medidas

Tomadas y propuestas por el responsable del tratamiento para:

- ▲ **Solucionar** la brecha.
- ▲ **Minimizar las consecuencias** sobre las personas.

### Contacto e identificación

- ▲ **Identificación comercial o pública** del responsable del tratamiento.
- ▲ Datos de contacto del **DPD u otro medio** de contacto para ampliar información.

## A tener en cuenta



#### No utilizar expresiones que distorsionen el mensaje.

como "Sus datos no están en riesgo", "no corre riesgo", "sus datos no se han visto afectados", "puede estar tranquilo, ya lo hemos denunciado a la AEPD"....

**No omitir detalles relevantes**, para que las personas puedan valorar el riesgo de forma adecuada y conforme a sus circunstancias particulares.

**No implica una única acción o acto.** Puede ejecutarse en distintas acciones atendiendo a la información que tenga el responsable sobre la magnitud de la brecha y las personas afectadas.

#### No es una comunicación a los afectados:

- ▲ Comunicar una brecha a una entidad o empresa cliente.
- ▲ Otros avisos o instrucciones para las personas que no incluyan el contenido mínimo del art. 34.
- ▲ Comunicado público injustificado, sin contenido mínimo o que no sea igualmente efectivo (web o portales corporativos no visitados por los afectados o similar).



Guía para la notificación de brechas de datos personales