What counts as a personal data breach?

Under the UK GDPR, a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data – whether due to accidental or deliberate causes or organisations failing to take appropriate action. So, it's a security incident that affects the confidentiality, integrity, or availability of personal data.

Some examples of possible data breaches include:

- an unauthorised third party accessing personal data;
- an organisation sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- the alteration of personal data without appropriate permission; and
- the loss of availability of personal data.

You can read more about this topic in our guidance: Report a breach | Personal data breach. There's also more information in our SME web hub.

Is it a personal data breach if an organisation sends someone's information to a previous address?

Not always.

In general, it's unlikely to be a breach – a type of security incident – when an organisation mails an old address it holds for someone if it reasonably believes that's still accurate (eg because the person hasn't updated their contact details).

A breach is also unlikely even where an organisation knows the person has moved but it still has a legal obligation in some situations to send certain correspondence to their 'last known address' – eg under the Consumer Credit Act 1974 [amended 2006] (CCA) (see: Is it a breach of the accuracy principle if someone receives correspondence or phone calls for another individual?). [LINK REMOVED – OUT OF SCOPE]

But a breach can happen if the organisation hasn't taken adequate security measures, or if they've not been properly followed – eg due to an employee accidentally sending mail to what's already been marked as an outdated address.

Organisations must put appropriate security measures in place that reflect the risks posed in the situation. For example, when considering mailing particularly sensitive information, the organisation may need to proactively adopt additional security measures like address verification or use a special courier service. In some cases, organisations may even decide that it's inappropriate to use the post at all, and explore alternative communication methods instead.

And even if there's no security breach, the organisation still needs to take appropriate steps to comply with the UK GDPR's data protection principles – including the accuracy principle. See: A guide to the principles | Does personal data always have to be up to date?

For more information on security breaches, see: Personal data breaches: a guide

Can inaccurate information lead to a personal data breach?

Yes – if the inaccuracy causes the integrity of the information to be compromised, and it leads to a security breach.

A breach of security can be described as an incident where there's been a failure to follow security obligations – it could be a process failure, or a lack of adequate measures being taken by an organisation.

Organisations must have processes in place to make sure the information they're handling is accurate - but accuracy issues won't always lead to a personal data breach, and need to be considered on a case-by-case basis.

For example, a doctor adding incorrect information to a patients record, when the information was given verbally by the patient, isn't a personal data breach.

However, if someone's prescription was entered onto the system incorrectly, and that resulted in the patient getting the wrong medicine, that's much more likely to be a personal data breach - because the integrity of the data's been compromised. In this scenario, the data isn't accurate for the purpose it's being processed - and organisational procedures should have prevented it from happening.

Is placing cookies on a device due to a technical failure a breach?

Yes – but only if they are non-essential cookies which haven't been consented to.

PECR requires consent for non-essential cookies. An organisation won't meet this requirement if it sets them when the user has not yet consented or has chosen to 'reject all'.

When setting cookies that involve personal data, the UK GDPR also applies. If a company uses or shares personal data collected by non-essential cookies without consent, this would be unauthorised. This is still the case if it's caused by a technical failure in the companies' cookie consent mechanism.

This would be a breach and it might be reportable, depending on what's happened.

What is a personal data breach under PECR and when should it be reported?

Under PECR, this is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service".

All service providers (organisations providing electronic communications services to the public, eg telecoms and internet service providers) must report personal data breaches to us within 24 hours of becoming aware of them (Reg 5A(2)). Service providers must also keep a breaches log and send it to us monthly.

Further, service providers must inform the subscriber (person named on the bill) or the user, if the breach adversely affects them without undue delay (Reg 5A(3)).

See our guidance: Direct marketing and PECR | PECR: a guide | Security breaches

There's also a useful flowchart to decide whether an organisation counts as a service provider in our old guidance: Notification of PECR security breaches (TNA archive). This guidance has now been withdrawn and should not be used as current guidance on breach reporting, but the flowchart (and section on service providers) may still be useful in some cases.

What counts as a breach of security under PECR?

There must have been a 'breach of security' leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise protected in connection with the provision of a public electronic communications service if that incident is to fall within the definition of a 'personal data breach' under PECR.

The key consideration when considering if a breach of security has occurred is whether the incident could have reasonably been prevented in view of the given circumstances. That is what could the service provider have reasonably done to prevent the incident occurring – which should be determined on a case-by-case basis.

For example, in a situation where a one off accidental human error results in an unauthorised disclosure, it's important to consider factors like:

- any measures the service provider could have implemented to prevent the unauthorised disclosure,
- given the associated cost, resource, and technical complexity of those measures, whether it was reasonable and appropriate in line with the risk of the disclosure occurring and severity of the implications of the disclosure, to expect the service provider to have implemented such measures, and
- whether those security measures would be proportionate in the particular circumstances.

You can read more about this topic in our PECR guidance on security of services, PECR guidance on security breaches and our notification of PECR security breaches guidance.

Is it a reportable breach if a whistleblowing employee takes information from their employer?

Not necessarily.

It might be if people's information is involved and if there's a risk to individuals.

If someone takes information about other employees from the organisation it could be considered an offence under section 170 of the DPA2018. Although, there may be a public interest defence in some cases.

A personal data breach involving a Section 170 offence should be assessed in the same way as any other personal data breach.

What's our position on using BCC to avoid disclosing personal email addresses?

While BCC can be a useful function, it's not enough on its own to properly protect people's sensitive information.

Organisations **must** have appropriate security measures to protect personal information in bulk emails. In some cases, revealing who's on an email list, or revealing personal contact details, could be particularly sensitive or harmful - even if there's no sensitive information in the main body of the email. We've seen a number of cases like this. Given the risk of human error, in such cases it's not enough to simply rely on staff using BCC.

So, if an email list might reveal sensitive information about the recipients (including but not limited to special category data), organisations **must** assess whether more secure methods would be appropriate (eg bulk email services or mail merge), to make sure details aren't shared by mistake.

If there's only a small number of recipients, they **could** consider sending individual emails instead.

Organisations should also train their staff on sending bulk emails.

Our new guidance for organisations is now live:

- UK GDPR | Email and security | BCC
- SME Web Hub | FAQs | Data storage, sharing and security | BCC

You may want to take a look at the following as well: SME web hub | Checklists | How well could you respond to a personal data breach? and Action we've taken | Incident types.

Are verbal disclosures a personal data breach?

Yes, assuming that it’s an unauthorised disclosure of recorded information.

As long as the UK GDPR applies to the information itself, any type of disclosure – including someone telling someone else – can be a personal data breach.

But don’t forget that the UK GDPR only applies if information's handled in an automated or structured way (or is intended to be handled in that way). For example, information that’s recorded in a digital system, or in organised paper files.

So if someone just repeats something they’ve heard, but that information isn’t actually recorded anywhere (and there’s no intent to record it) then it’s not a breach – because the UK GDPR won’t apply.