Notification of PECR security breaches

Privacy and Electronic Communications Regulations

Contents

Introduction

1. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by telephone, fax, email, text and picture or video message, or by using an automated calling system. PECR also include other rules relating to cookies, telephone directories, traffic data, location data and security breaches.

2. An overview of the main provisions of PECR can be found in The Guide to Privacy and Electronic Communications.

3. This is part of a series of guidance, which goes into more detail than the Guide, to help organisations fully understand their obligations and promote good practice.

4. This guidance explains to organisations who provide electronic communications services to the public when and how to notify the ICO about a security breach.

Overview

- This guidance applies to organisations providing electronic communications services to the public (eg telecoms providers and internet service providers).
- Service providers must notify the ICO that a personal data breach has occurred within 24 hours of becoming aware of the basic facts. Full details must be provided as soon as possible. The ICO provides a secure online form for all notifications.
- If the breach is likely to adversely affect individuals, the service provider must also notify those individuals without undue delay.
- Service providers must also keep a log of any breaches, and should submit this to the ICO on a monthly basis.

Relevant security breaches

5. Under regulation 5A of PECR, 'service providers' have a specific obligation to notify the Information Commissioner – and in some cases their own customers – about a 'personal data breach'. They are also required to keep a log of those breaches.

What is a 'service provider'?

6. In essence, a service provider is someone who provides any service allowing members of the public to send electronic messages. It will include telecoms providers and internet service providers.

7. Regulation 5(1) of PECR defines a service provider as *"a provider of a public communications service".* Regulation 2 incorporates further relevant definitions from the Communications Act 2003.

8. A public communications service is defined in section 151 of the Communications Act 2003 as *"any electronic communications service that is provided so as to be available for use by members of the public".* What constitutes electronic communications is further defined in section 32 – in short, any electrical, magnetic or electro-magnetic signals (including speech, music, sounds, visual images or data of any description) conveyed over a transmission system.

9. However, the definition excludes 'content services'. Section 32(7) of the Communications Act 2003 defines a content service as:

> "so much of any service as consists in one or both of the following—
>
> (a) the provision of material with a view to its being comprised in signals conveyed by means of an electronic communications network;
>
> (b) the exercise of editorial control over the contents of signals conveyed by means of such a network."

10. So, for example, a shopping portal or an online newspaper would be a content service, and not an electronic communications service.

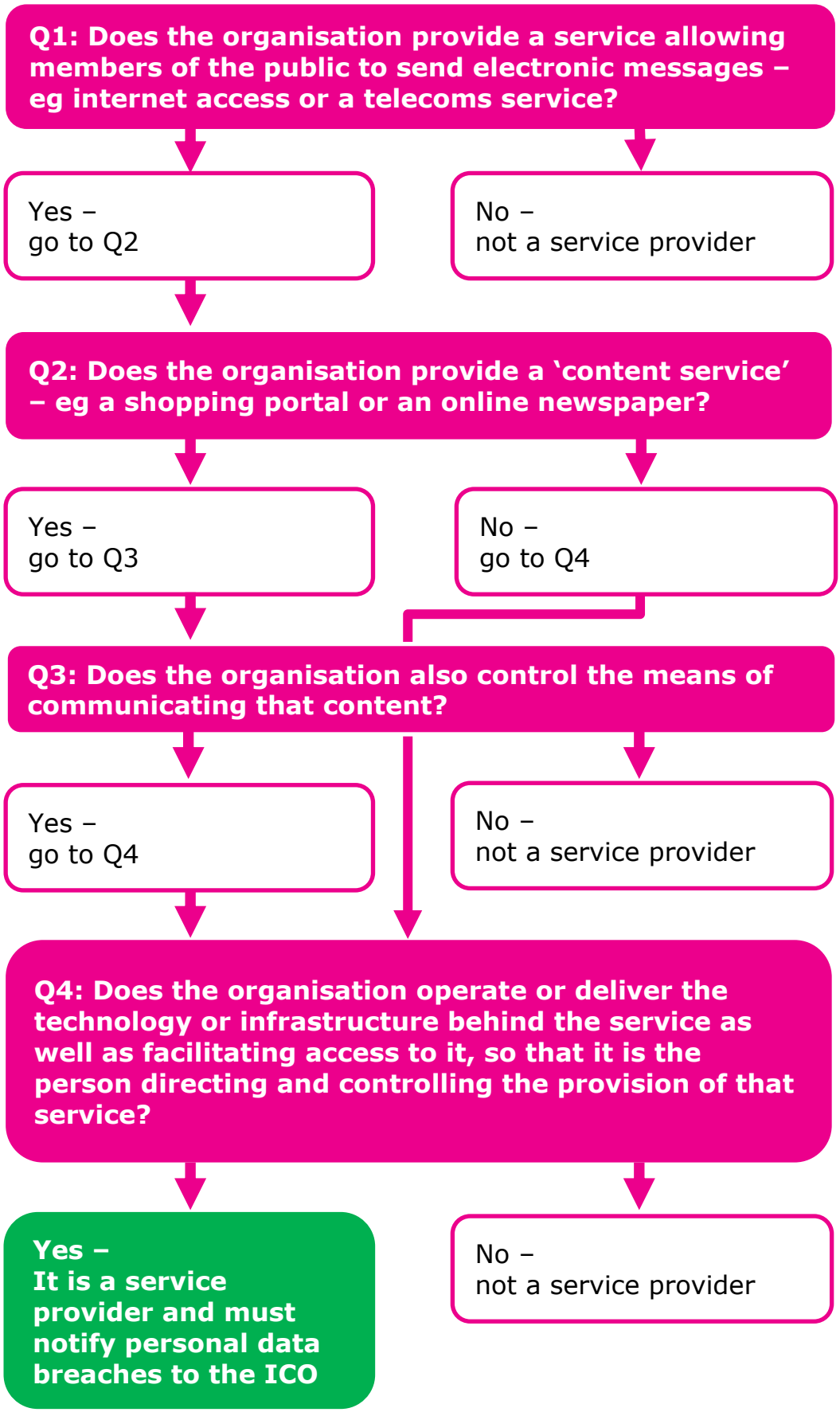
11. Organisations will therefore need to consider a range of factors to determine whether they are service providers with notification obligations under PECR. Any organisation which meets the following criteria is likely to be a service provider:

    - it provides a service which transmits electronic signals (and is not purely providing content);
    - the service is available to members of the public;
    - the service is provided as a primary activity, rather than as a supplementary service such as wi-fi provided in a pub or on a train; and
    - if there are multiple organisations involved in providing the service, this organisation directs and controls the provision of service to the end user.

12. This is not intended to be an exhaustive list, and organisations will need to give full consideration to their own specific circumstances. The flowchart on the next page summarises the steps organisations need to go through to determine whether they are service providers, and therefore whether they are required to notify personal data breaches to the ICO.

13. It is useful to remember that the purpose of these provisions is to protect individuals' data and privacy in the context of their electronic communications. Therefore it is important for organisations to consider the type of personal data they hold and whether any security breach could adversely affect an individual – for example, by causing financial loss, reputational damage or identity fraud. If an organisation does not hold this type of data, it is unlikely to be caught by these provisions.

14. If an organisation is responsible for delivering part of the service but does not have a direct contractual relationship with end users, it does not have to notify the ICO of a personal data breach – but it must immediately notify the organisation that does have the contractual relationship with end users, and that organisation must then notify the ICO.


Q1: Does the organisation provide a service allowing members of the public to send electronic messages – eg internet access or a telecoms service?
Yes – go to Q2
No – not a service provider
Q2: Does the organisation provide a 'content service' – eg a shopping portal or an online newspaper?
Yes – go to Q3
No – go to Q4
Q3: Does the organisation also control the means of communicating that content?
Yes – go to Q4
No – not a service provider
Q4: Does the organisation operate or deliver the technology or infrastructure behind the service as well as facilitating access to it, so that it is the person directing and controlling the provision of that service?
Yes – It is a service provider and must notify personal data breaches to the ICO
No – not a service provider

What is a 'personal data breach'?

15. A personal data breach is defined in PECR as:

> "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".

16. In short, there will be a personal data breach whenever any personal data is accidentally lost, corrupted or disclosed, or if someone accesses it or passes it on without proper authorisation.

17. A personal data breach is broadly defined as an incident which affected the availability, integrity or confidentiality of the personal data. This therefore includes a network intrusion by an unauthorised third-party and also a deliberate or accidental action by the service provider. For example, an employee causing the unintended deletion of personal data and no appropriate back-up exists would constitute a personal data breach. There is no threshold for how serious the breach must be – all breaches must be notified.

18. More information on what exactly constitutes 'personal data' is available on our guidance pages.

Breaches of encrypted information

19. If the personal data was encrypted to an appropriate standard, and the decryption key remains secure, service providers should strictly speaking still notify us of the breach. However, the ICO is unlikely to take formal enforcement action against an organisation that fails to notify us of a breach if the information was properly encrypted and remains secure.

Notifying the ICO

20. Regulation 5A(2) of PECR states:

> **5A.**—(2) If a personal data breach occurs, the service provider

> shall, without undue delay, notify that breach to the Information Commissioner.

21. From 25 August 2013, European Commission Regulation 611/2013 (the Notification Regulation) sets out further rules about exactly how and when to notify, and what the notification must contain. Service providers must now notify the ICO of any personal data breach within 24 hours of detection.

Within 24 hours of detection

22. Article 2(2) of the Notification Regulation states:

> The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible.
>
> The provider shall include in its notification to the competent national authority the information set out in Annex I.
>
> Detection of a personal data breach shall be deemed to have taken place when the provider has acquired sufficient awareness that a security incident has occurred that led to personal data being compromised, in order to make a meaningful notification as required under this Regulation.

23. In other words, service providers must tell us within 24 hours of becoming aware that a personal data breach has occurred. As soon as they have enough information to confirm that there has been a breach and provide some basic facts, they must notify, even if they can't yet provide full details.

24. We do accept that in many cases it will not be feasible to provide us with full details within 24 hours. In such cases, article 2(3) of the Notification Regulation requires that service providers should still make an initial notification within 24 hours, essentially just to tell us that they have detected a breach. They should then follow this up with a second notification within three days of the initial notification, to provide further information.

25. If the service provider still cannot provide full details within that extra three days, it should still submit the second

notification with as much information as possible, together with a reasoned justification for the further delay. It should then send us the remaining information as soon as possible.

26. We accept that service providers may need to undertake an investigation to understand exactly what has happened and what needs to be done to mitigate the breach, and that in many cases this will take longer than three days. However, they must still notify us of the existence of the breach within 24 hours, and submit a second notification within three days justifying any further time required to investigate. We will expect service providers to prioritise the investigation, to give it adequate resources, and expedite it as a matter of urgency. They must provide us with any missing details as soon as they have completed their preliminary investigations – we would expect that this should not normally take longer than two weeks.

What information to include

27. The initial notification (within 24 hours) must always include the following summary information:

- The name of the service provider.
- The name and contact details of the data protection officer or other contact point where more information can be obtained.
- Whether it is an initial notification or a full notification.
- The date and time of the breach (or an estimate) and the date and time of detection.
- The circumstances of the breach (eg theft, loss, copying).
- The nature and content of the personal data concerned.
- Technical and organisational measures applied (or to be applied) to the affected personal data.
- Relevant use of other providers (where applicable).

28. If possible, the initial notification should also include the more detailed information set out below. Otherwise, this should be included in the second notification, or as soon as possible after that:

- A summary of the incident that caused the breach, including the physical location of the breach and the storage media involved.
- The number of individuals concerned.
- The potential consequences and potential adverse effects on those individuals.
- The technical and organisational measures taken to mitigate those potential adverse effects.
- The content of any notification to customers.
- The means of communication used to notify customers.
- The number of customers notified.
- Whether the breach affects individuals in other EU member states.
- Any notification of other data protection authorities.
- If all these details cannot be included in the second notification, a reasoned justification for the further delay.

29. In line with the Notification Regulation, we now provide a secure PECR security breach notification web form for service providers to use to notify us of breaches. Additional documents can be attached to this form if necessary.

What happens next

30. We will consider the information provided to assess whether the service provider is complying with its obligations under PECR, including the duty to take appropriate technical and organisational measures to safeguard the security of its service, the duty to notify us of a breach, and the duty to notify customers of breaches adversely affecting their privacy.

31. We will contact service providers within two weeks of their notification to indicate what the next steps will be.

Notifying customers

32. Regulation 5A(3) of PECR states:

> **5A.**—(3) Subject to paragraph (6), if a personal data breach is likely to adversely affect the personal data or privacy of a subscriber or user, the service provider shall also, without undue delay, notify that breach to the subscriber or user concerned.

33. In other words, service providers must also notify their customers if the breach is likely to adversely affect them.

If a breach is likely to adversely affect them

34. Whether the breach is likely to adversely affect individuals is primarily a decision for the service provider, based on the circumstances of the case. Service providers should consider the following factors:

    - the nature and content of the personal data.
    - whether it includes sensitive personal data, as defined in the DPA, or other details people might consider intrusive – especially financial information, location data, internet log files, web browsing histories, email data or itemised call lists.
    - what harm could be caused to the individual – and in particular whether there is a threat to physical safety or reputation or a risk of identity theft, fraud, financial loss, psychological distress or humiliation.
    - who now has access to the data, to the extent this is known.

35. A service provider does not have to notify customers if the Information Commissioner confirms that he is satisfied the information was properly encrypted when the breach occurred.

What to tell customers

36. Any notification to customers must include the following information:

- The name of the service provider.
- The name and contact details of the data protection officer or other contact point where more information can be obtained.
- A summary of the incident causing the breach.
- The estimated date of the incident.
- The nature and content of the personal data concerned (and in particular whether it included sensitive personal data, financial information, location data, internet log files, web browsing histories, email data or itemised call lists).
- The likely consequences of the breach on the individual concerned (and in particular whether there is a risk of identity theft or fraud, physical harm, distress or damage to reputation).
- Measures taken by the provider to address the breach.
- Measures the individual could take to mitigate any possible adverse effects of the breach.

37. We recommend that the notification includes a helpline number or web address if possible. It must be in clear and simple language, and must not include any marketing messages or other content. In particular, it should give clear, specific advice on steps the individuals can take to protect themselves from harm, and explain what the service provider is willing to do to assist them.

When and how to notify customers

38. Service providers must notify affected customers without undue delay – in other words, as soon as they have sufficient information about the breach. If doing so would put a proper investigation of the breach at risk, a service provider can ask

the ICO to approve a delay in notification until it has completed its investigation.

39. The means of communication should be prompt and secure. It should be a specific message about the breach, and not be combined with a communication on another topic.

Keeping a log of security breaches

40. Service providers are also required to keep a log of security breaches. Regulation 5A(8) of PECR states:

> **5A.**—(8) Service providers shall maintain an inventory of personal data breaches comprising—
>
> (a) the facts surrounding the breach,
>
> (b) the effects of the breach, and
>
> (c) remedial action taken
>
> which shall be sufficient to enable the Information Commissioner to verify compliance with the provisions of this regulation. The inventory shall only include information necessary for this purpose.

41. We have produced a template log to help you record the information you need. To ensure that all breaches have been properly notified to us, service providers should submit their completed log to us on the first working day of each month. As with breach notifications, completed logs should be submitted using our secure notification form. Service providers should simply select the 'completed monthly log' option and attach a copy of their log.

42. If there have not been any personal data breaches in a particular month, service providers can email us at datasecuritybreach@ico.org.uk to confirm a 'nil return'. As nil returns do not have to be sent securely, there is no need to use the online form.

43. Strictly speaking, PECR does not require this monthly return. However, we believe that this remains a useful exercise as it will demonstrate that service providers are monitoring their security properly and taking their responsibilities seriously. If

we do not receive a monthly return from a service provider, this may trigger further investigation.

44. We will also inspect logs of personal data breaches during PECR audits. We will use the logs and any other relevant information that comes to our attention to check that service providers are complying with their obligations under PECR, including the duty to maintain a log and notify us of any personal data breaches.

45. As the ICO is subject to the Freedom of Information Act, we may receive requests for a service provider's logs and associated information. We will take the service provider's views into account when considering any request.

46. We will usually keep the logs for two years; longer if the information leads to us taking formal regulatory action. We will also retain a summary record for as long as is necessary to help inform our future work, but no individuals will be identifiable from this record. However, service providers may need to keep their logs for longer than this for their own business purposes.

More information

48. Additional guidance is available on our guidance pages with more information on other aspects of PECR and the Data Protection Act.

49. This guidance has been developed drawing on ICO experience. Because of this it may provide more detail on issues that are often referred to the ICO than on those we rarely see. The guidance will be reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.

50. It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

51. If you need any more information about this or any other aspect of PECR, please contact us: see our website www.ico.org.uk.