Enforcing the revised Privacy and Electronic Communications Regulations (PECR)

What is changing?

On 26 May 2011, the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 come into force. These amend the Privacy and Electronic Communications (EC Directive) Regulations 2003. The Information Commissioner already has enforcement powers under the 2003 Regulations. The 2011 Regulations enhance these powers and introduce new requirements, most notably in relation to cookies.

The Commissioner will continue to use his existing powers to address complaints about contraventions of the 2003 Regulations and enforce these Regulations. The purpose of this note is to explain how the Information Commissioner will approach:

- the use of his new powers to enforce the requirements of the 2003 Regulations; and
- the use of his powers to enforce the new requirements introduced by the 2011 Regulations.

The Commissioner has discretion over if, how and when he uses his enforcement powers. He does though have to act within the limits of reasonableness and can be subject to judicial review if he does not. He also has to recognise that the Regulations have been drawn up by the Government, laid before Parliament and directly implement an EU Directive. They are the law and there is an expectation that broadly, he will enforce them.

What are the Commissioner's new powers?

The new powers enable the Commissioner to:

- impose civil monetary penalties of up to £500,000 for serious breaches of PECR;
- audit the measures taken by a provider of public electronic communications services (a service provider) to:

- safeguard the security of that service

- comply with the new personal data breach notification and recording requirements

- impose a fixed monetary penalty of £1,000 on a service provider that fails to comply with the new breach notification requirements; and

- require a communications provider to provide him with information needed to investigate the compliance of any person with PECR (a third party information notice).

How will the Commissioner approach the use of his powers?

The Commissioner will, subject to the provisions of this note, continue to follow the approach set out in his Data Protection Regulatory Action Policy. This means adopting a targeted, risk-driven and proportionate approach to the use of his powers. It also means being selective with the key driver for action being concerns about significant actual or potential detriment caused to individuals by a failure to comply with the requirements of PECR.

Using the new powers

Civil monetary penalties

The use of this power is limited to circumstances where:

- there has been a serious contravention of PECR; and

- the contravention was of a kind likely to cause substantial damage or substantial distress; and

- the contravention was deliberate or the person responsible knew or ought to have known that a contravention would occur and failed to take reasonable steps to prevent it.

The circumstances in which it is appropriate to serve a monetary penalty will be limited. The Commissioner does though take the view that the requirement to demonstrate the potential for "substantial damage or substantial distress" can be met by contraventions where the damage or distress to any one individual is more limited but large numbers of individuals are affected. Thus there is the potential to impose monetary penalties for serious

contraventions of the PECR provisions relating to the sending of unsolicited marketing messages.

The Commissioner is required to issue guidance on how he proposes to exercise his powers to impose civil monetary penalties. Now that the power has been extended to contraventions of PECR he will have to revise his existing guidance. The revised guidance will follow broadly the same approach as the current guidance. The revised guidance has to be approved by the Secretary of State and laid before Parliament before it can be issued. In addition the Commissioner will consult those likely to be affected by the revised guidance. This means that the revised guidance is unlikely to be issued before October 2011.

The Commissioner does not intend to impose any civil monetary penalties for PECR contraventions until the revised guidance has been issued. In any case he is not able to impose penalties for breaches that took place before the coming into force of the 2011 Regulations on 26 May 2011. The Commissioner may nevertheless start to gather evidence of non compliance from 26 May 2011 onwards for future use in connection with the imposition of civil monetary penalties. Furthermore, and subject to the provisions of this note, there is still the possibility of the Commissioner using his existing enforcement powers in connection with PECR contraventions. His new third party information notice powers will be available to assist him with this.

Audit

The new audit powers enable the Commissioner to undertake audits without necessarily having the consent of a service provider. Nevertheless the Commissioner will maintain his commitment to normally seeking the agreement of a service provider to a consensual audit in the first instance. Only where the service provider is unwilling to engage and risks to privacy have been identified will he use his power to conduct a compulsory audit.

The Commissioner will develop more detailed guidance on the use of his new audit power. This will involve discussions with service providers. The Commissioner does not envisage conducting any audits under the new provisions until this guidance is published. It should though be noted that this new audit power differs from the Commissioner's assessment notice power under section 41A of the Data Protection Act 1998 in that the Commissioner is not prevented from imposing a civil monetary penalty for contraventions he finds in the course of a compulsory audit under the 2011 Regulations.

Fixed monetary penalties

The Commissioner does not consider that service providers need a lengthy period in which to implement the new breach notification requirements. Following consultation with service providers, he will be issuing guidance on their detailed application, but the basic requirements are clear from the 2011 Regulations. They are also in line with the voluntary breach notification system currently operated by the Commissioner. The Commissioner does not consider that a lead in period of any more than one month following 26 May 2011 is needed before service providers become liable to fixed monetary penalties. Service providers should be aware that the Commissioner is not prevented from imposing a fixed monetary penalty where a contravention is discovered in the course of an audit. However he has discretion, based on the circumstances of the case, as to whether he imposes a fixed monetary penalty when he becomes aware of a contravention. He also has discretion as to whether, when multiple contraventions are discovered he imposes a single penalty or multiple penalties.

Third party information notices

The Commissioner will make use of this new power from 26 May 2011 in appropriate cases.

Enforcing the new requirements

Revised rules for cookies

The revised rules replace the requirement of the 2003 Regulations that users must be given an opportunity to refuse cookies (an "opt out") with a requirement for user consent. The requirement to also provide users with clear, comprehensive information on the use of cookies remains. In fact these requirements do not only apply to cookies. They apply to any means of storing information or gaining access to information stored on a user's terminal equipment. They do not apply where the storage or access is strictly necessary for a service requested by the user.

The Commissioner recognises that, in many cases, implementation of the rule requiring consent for cookies will be challenging for organisations. He has issued separate advice on how these requirements might be met in practice. Immediate implementation could though significantly restrict the operation of internet services that users generally take for granted. It would be likely to cause

disproportionate inconvenience both to website providers and to users.

Nevertheless implementation is required. The Commissioner cannot exempt organisations from the requirements of the Regulations. He will though allow a lead in period of 12 months for organisations to develop ways of meeting the cookie related requirements of the 2011 Regulations before he will move towards the approach set out in his Data Protection Regulatory Action Policy and consider using his enforcement powers to compel them to do so in appropriate cases. This lead in period will end in May 2012.

In allowing this lead in period the Commissioner has born in mind the position stated by the Government in its response to its consultation on Implementing the revised EU Electronic Communications Framework that:

- it does not expect work on technical solutions to be completed before the implementation deadline;
- it recognises that it will take time for these solutions to be developed, evaluated and rolled out; and
- during this time it does not expect that ICO will take enforcement action against organisations that are working to address their use of cookies or are engaged in development work on browsers and/or other solutions.

The Commissioner has also born in mind that when the 2003 Regulations were made there was a three month delay before they came into effect. In addition "good regulation" requires that guidance on implementation needs to be available to organisations at least 12 weeks before new regulations come into effect. In the absence of other guidance from the Government it is the Commission's advice note, Changes to the rules on using cookies and similar technologies for storing information that fulfills this requirement. This advice note could not be issued before early May 2011 when the 2011 Regulations were published. Furthermore the Commissioner is aware that the UK is ahead of most other EU member states in implementing the EU Directive that sits behind the 2011 Regulations.

The Commissioner does not though condone organisations taking no action in the period up to May 2012. Organisations should be taking steps to ensure they can properly comply with the revised rules for cookies by May 2012. If it appears to the Commissioner that particular organisations are not making adequate preparations to be

compliant by May 2012 he may issue them with a warning as to the future use of his enforcement powers. In the event of complaints being received after May 2012 any such warnings will be taken into account by the Commissioner in deciding if and when to issue an organisation with an enforcement notice.

From May 2012 onwards the Commissioner will follow the approach to enforcement set out in his Data Protection Regulatory Action Policy. This means that in deciding whether to take enforcement action in relation to a breach of the revised cookies rules he will be concerned with the impact of the breach on the privacy and other rights of website users and not just with whether there has been a technical breach of the 2011 Regulations.

In the meantime it is nevertheless likely that the Commissioner will receive complaints about cookies. Initially, where those complaints indicate non compliance with the 2011 Regulations, he will provide advice to the organisation concerned on the requirements of the law and how they might comply. Where he considers it appropriate, and particularly as May 2012 approaches, he will also ask organisations to explain to him the steps they are taking to ensure that they will in fact be in a position to comply by May 2012.

The Commissioner will of course continue to consider complaints about contraventions of the requirement in the 2003 Regulations that information is provided to users about cookies. He will continue to enforce this requirement in appropriate cases.

Security of services

The Commissioner does not consider that the specific security requirements introduced in the 2011 Regulations place significant additional obligations on service providers. They are consistent with the steps the Commissioner would expect service providers to be taking already to meet the more general requirements of the 2003 Regulations. The Commissioner's existing enforcement powers will therefore apply fully to these requirements from 26 May 2011. How his new civil monetary penalty and audit powers will be applied to these requirements is discussed above.

Personal data breach notification

The application of the Commissioner's new powers to the personal data breach notification requirements is discussed above. To the extent that the application of the Commissioner's existing enforcement powers is relevant in this context he will allow the same one month lead in period following 26 May 2011. Service

providers should be aware that, apart from the qualifications discussed in this note, notification of a personal data breach to the Commissioner does not remove them from potential liability for civil monetary penalty.

Access for national security, legal requirements, law enforcement etc.

The 2011 Regulations require communications providers to establish internal procedures for responding to requests for access to users' personal data for the above purposes. They also require communications providers to, on demand, provide information to the Commissioner about these procedures, the number and nature of requests received and their response to them.

The Commissioner understands that some communications providers may not yet have the necessary internal procedures in place for responding to such requests. Establishing such procedures will take some time. The Commissioner therefore intends to allow a lead in time of three months before considering the possible use of his enforcement powers in connection with these requirements. Similarly he would not envisage placing any demands on communications providers for the information he is entitled to under the 2011 Regulations before August 2011.