EE

Privacy and Electronic Communications Regulations audit report

Executive summary
May 2018

Information Commissioner's Office

1. Background and Scope

The Information Commissioner may audit the measures taken by the provider of a public electronic communications service (service provider) to safeguard the security of that service (Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 Reg. 5(6)).

The Information Commissioner sees auditing as a constructive process with real benefits for service providers and so aims to establish, wherever possible, a participative approach.

In August 2017, EE agreed to a consensual audit by the ICO of its public electronic communications service. An introductory meeting was held with representatives of EE to identify and discuss the scope of the audit.

The audit scope was the compliance with Regulation 5 of the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011; in particular, the extent to which a service provider has taken appropriate technical and organisational measures to safeguard the security of the service.

The audit was conducted following the Information Commissioner's Privacy and Electronic Communications Regulations audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

The audit field work was undertaken at BT Centre in London, and at EE's contact centre in Darlington and at six EE retail stores in London and Manchester between 19 and 22 March 2018.

2. Audit Approach

The audit was conducted following the Information Commissioner's Privacy and Electronic Communications Regulations (PECR) audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

The purpose of the audit was to provide the Information Commissioner and EE with an independent assurance of the extent to which EE, within the scope of this agreed audit, is complying with the PECR.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with the PECR.

In order to assist data controllers in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. These ratings are assigned based on the following risk matrix:

Impact					
	Severe	High	High	Urgent	Urgent
	High	Medium	Medium	High	Urgent
	Medium	Low	Medium	Medium	High
	Low	Low	Low	Medium	High
		Remote	Unlikely	Likely	Very Likely
		Likelihood			

It is important to note that the above ratings are assigned based upon the ICO's assessment of the risks involved. EE's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

3. Audit grading

Audit reports are graded with an overall assurance opinion, and any issues and associated recommendations are classified individually to denote their relative importance, in accordance with the following definitions.

Colour code	Internal audit opinion	Definitions
	High assurance	There is a high level of assurance that processes and procedures are in place and are delivering PECR compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with the PECR.
	Reasonable assurance	There is a reasonable level of assurance that processes and procedures are in place and are delivering PECR compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with the PECR.
	Limited assurance	There is a limited level of assurance that processes and procedures are in place and are delivering PECR compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the PECR.
	Very limited assurance	There is a very limited level of assurance that processes and procedures are in place and are delivering PECR compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

4. Audit opinion

The primary purpose of the audit is to provide the Information Commissioner and EE with an independent opinion of the extent to which EE, within the scope of this agreed audit, is complying with Regulation 5 of the PECR.

The recommendations made are primarily around enhancing existing processes to facilitate compliance with Regulation 5 of the PECR.

Overall Conclusion	
High Assurance	The technical and organisational measures taken by the provider of a public electronic communications service to safeguard the security of that service provide a high level of assurance that processes and procedures are in place and being adhered to. The audit has identified limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance.

5. Summary of Recommendations

Urgent Priority Recommendations – These recommendations are intended to address risks which represent clear and immediate risks to the service provider's ability to comply with the requirements of the PECR.	We have made 0 urgent priority recommendations where controls could be enhanced to address the issues identified.
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of the PECR.	We have made 0 high priority recommendations where controls could be enhanced to address the issues identified.
Medium Priority Recommendations - These recommendations address risks which can be tackled over a longer timeframe or where mitigating controls are already in place, but which could be enhanced.	We have made 3 medium priority recommendations where controls could be enhanced to address the issues identified.
Low Priority Recommendations - These recommendations represent enhancements to existing good practice or where we are recommending that the service provider sees existing plans through to completion.	We have made 2 low priority recommendations where controls could be enhanced to address the issues identified.

6. Summary of audit findings

Areas of good practice

EE have a robust inspection regime for their Retail Stores, with regular and risk-assessed inspections of sites to test and support local compliance with security and privacy expectations.

EE are in the process of rolling out an improved point of sale system across their retail estate which will reduce and eventually remove the local storage of paper records.

EE demonstrated a data landscaping tool which has been developed as a part of the BT Group's GDPR preparations. This platform provides a detailed and granular record of assets and the nature of their data and processing including aspects such as consent, location, access, transfers, suppliers, protection, segregation, and other security and privacy aspects.

EE have strong project management procedures in place which embed security and privacy concepts and ensure oversight and signoff by specialist security staff.

Staff have their knowledge of policies and procedures reinforced by well-developed training resources, including a 'Digital Academy' platform accessible from staff's own mobile devices. Training completion is very high, and a mandatory training board keeps training under review and enables iterative development and rapid changes if necessary.

Areas for improvement

EE employs three different access card systems across its sites, but with differing levels of control over flagging failed access attempts, open door alarms, and maintaining an audit trail.

The transition of EE from their legacy T-Systems assets and managed services to BT resources provides an opportunity to reconcile personal data-processing assets with BT's in-house asset management tools and mechanisms across the estate.

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate security arrangements in place rests with the management of EE.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.