

# PRIVACY HORIZONS: TERRA INCOGNITA

29<sup>th</sup> International Conference of  
Data Protection and Privacy Commissioners

September 25 to 28, 2007  
Montreal, Canada



## LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE : TERRA INCOGNITA

29<sup>e</sup> Conférence internationale des commissaires  
à la protection des données et de la vie privée

du 25 au 28 septembre 2007  
Montréal, Canada

# Data Protection Auditing A UK Perspective

Chris Turner

Head of Audit & Remedies

Information Commissioner's Office

# Background

- **1998 Data Protection Act – Provides a power to audit with consent of the data controller.**
- **Mid 2001 Completion of Audit Manual and promotion via our website – A major milestone for the Office.**
- **Late 2003 new initiative launched to undertake programme of trial audits and consider audit accreditation schemes.**
- **Audits conducted by compliance team members.**
- **May 2005 permanent Audit Team created as part of a new Regulatory Action Division.**
- **2007 looking to expand team and increase powers.**

# Audit Programme

- **Programme based on:**
  - **Volunteers**
  - **Theme**
  - **Identified Non Compliance / Issues**
- **Engagement**
  - **Invitation / Request**
  - **Assessment / Remedies**
  - **Undertaking**
- **Make Up**
  - **Predominantly public authorities, private companies more likely to be as a result of undertakings.**

# Audit Methodology

- **Based broadly on the Audit Manual**
- **2/3 man team, compliance background experience**
- **Development of key relationships to facilitate co-operation and establish mutual benefits**
- **Scoping and planning (background information)**
- **Adequacy Audit**
  - **Policies, Procedures, Guidelines, Training Material**
  - **Checklist Evaluation**
- **Compliance Audit**
  - **Data Protection System**
  - **Business (Functional) Processes**
  - **Computer applications / operations**

# Audit Output

## ICO Methodology

- **Adequacy Audit**
  - **Summary Report**
  - **Observations Report (Working document)**
- **Compliance Audit**
  - **On-site Feedback (key findings)**
  - **Compliance Report (Observations / Evaluation / Recommendations)**
- **Follow up**

# Challenges

- **No audit without consent**
- **Team Experience (Audit / Technical)**
- **Questionnaire approach – getting the questions right.**
- **Availability of adequate background information e.g. process / job descriptions**
- **Getting the timetable right!**
- **‘Deep and Narrow’ v ‘Wide and Shallow’**
- **Reports & Recommendations**
- **Balancing the workload – Small team considerations**

# Benefits

## ICO

- **Opportunity to identify / address systemic issues.**
- **Provides an alternative to enforcement.**
- **Increased ICO understanding of processing.**
- **Identifies the need for guidance.**
- **Raise the profile of data protection.**

## Organisations

- **Raise data protection awareness at an individual and corporate level.**
- **Provides a perspective of the regulator's view**
- **Is a catalyst for change.**
- **Provides an alternative to enforcement.**