



---

# **Google Inc.**

## **Data Protection Audit Report**

### **Executive Summary**

**August 2011**

---

---

## 1. Background

- 1.1 The Information Commissioner may, with the consent of the data controller, assess the extent to which good practice is applied when processing personal data and shall inform the data controller of the results of the assessment. (Data Protection Act (DPA) 1998 s51 (7))
- 1.2 The Information Commissioner sees auditing as a constructive process with real benefits for data controllers and so aims to establish, wherever possible, a participative approach. (Assessment Notice Code of Practice 2.1)
- 1.3 An Assessment Notice is the medium through which the Information Commissioner's Office (ICO) will seek to instigate a compulsory audit. However, the Assessment Notice Code of Practice, in the interests of clarity, distinguishes between compulsory and consensual audits. (Assessment Notices Code of Practice, 2.1, Para 6 & Appendix A.)

The Information Commissioner has reiterated a desire, in the first instance and as far as is practicable, to conduct consensual data protection audits.

- 1.4 In 2010, the Information Commissioner became aware by means of a public Google blog, that Google Street View vehicles, which had been adapted to collect publicly available wi-fi radio signals, had mistakenly collected a limited amount of payload data, likely to include a very limited quantity of emails, URLs and passwords.
- 1.5 Google's purpose had been to identify wi-fi networks and to map their approximate location using GPS co-ordinates of the GSV car when the radio signal was received. The aim was to build and improve the geo-location database for location-based mobile applications.
- 1.6 The Commissioner considered the data controller's compliance with the provisions of the Act in light of this matter and, following consideration of the remedial action taken by Google Inc. and the evidence available, decided to not exercise his enforcement powers.
- 1.7 In consideration of this, Google Inc. signed an undertaking in November 2010 confirming the steps it would take to ensure that personal data is processed in accordance with the first principle in Part 1 of Schedule 1 to the Act. (the "Undertaking")
- 1.8 Within the Undertaking, Google Inc. agreed, within nine months from the date of the undertaking, to facilitate a consensual audit by the ICO, the objective, framework and scope of which was set out in

Schedule 1 of the undertaking. Schedule 1 of the undertaking is attached as Appendix 1 for reference.

---

## **2. Scope of the Audit**

- 2.1 The audit will review the confidential written Privacy Report as provided by Google Inc to the Information Commissioner, which will detail Google's implementation of the privacy processes it outlined on October 22, 2010 in a blog posted by Alan Eustace, as applied to Google's UK operations as such processes are set in the Undertaking. The Privacy Report will cover the areas set out in Appendix 1 below.

The audit will validate the Privacy Report's accuracy and findings.

---

### 3. Audit Opinion

3.1 The primary purpose of the audit is to provide the Information Commissioner and Google Inc. with an opinion to the extent to which Google Inc. has complied with the terms of the Undertaking.

Overall Conclusion	
Reasonable assurance	<p>The audit has provided reasonable assurance over the accuracy and findings of the Privacy Report as provided by Google Inc. to the Information Commissioner. It has also provided reasonable assurance that Google have implemented the privacy process changes outlined in the Undertaking.</p> <p>The audit has identified some scope for improvement in existing arrangements and appropriate action has been agreed.</p> <p>The audit verified that Google have made improvements to their internal privacy structure, privacy training and awareness and privacy reviews. The audit provided reasonable assurance that these changes reduce, but do not eliminate, the risk of an incident similar to the mistaken collection of payload data by Google Street View vehicles occurring again.</p>

## 4. Audit Grading

4.1 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 definitions in the table below.

<b>Colour Code</b>	<b>Internal Audit Opinion</b>	<b>Recommendation Priority</b>	<b>Definitions</b>
	High assurance	Minor points only are likely to be raised	The arrangements for data protection compliance with regard to governance and controls 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.
	Reasonable assurance	Low priority	The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements.
	Limited assurance	Medium priority	The arrangements for data protection compliance with regard to governance and controls provide only limited assurance that processes and procedures are in place and are being adhered to. The audit has identified scope for improvement in existing arrangements
	Very Limited assurance	High priority	The arrangements for data protection compliance with regard to governance and controls provide very limited assurance that processes and procedures are in place and being adhered to. There is therefore a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

---

## 5. Summary of Audit Findings

### 5.1 Areas of Good Practice.

- Google have developed an internal privacy structure with both privacy focussed teams and cross functional groups responsible for evaluating and reviewing the privacy aspects of projects. Privacy focussed teams include the Privacy Engineering Team, led by Dr Alma Whitten, which has responsibility for developing and maintaining privacy processes and the Privacy Legal Team, which provides privacy specific legal guidance to the company. Cross functional groups which form part of the privacy review process for projects include the Privacy Working Group and First Level Review Team and these both consist of both technical and non technical members. All of these teams work across product, engineering, legal and compliance functions. The development of both privacy focussed teams and the introduction of cross functional teams working on privacy marks an increase in resource dedicated to, and visibility of, privacy at Google.
- Training for both new and existing employees has been enhanced, and incorporates practical examples drawn from real life situations to demonstrate the practical implications and application of privacy.
- Google have developed and delivered online, mandatory training for all staff on the Google Code of Conduct, which covers privacy and the protection of user data, and Information Security Awareness training in order to increase business wide awareness of their privacy principles. This training also enables awareness amongst employees of their obligations and responsibilities with regards to privacy. In addition, orientation training ensures all new employees receive training on Google's privacy principles, while new engineers also receive additional privacy specific technical training as part of their induction.
- Advanced Data Protection Training has been developed for all engineers and Google have developed a range of initiatives such as TechTalks, training videos and poster campaigns to raise the profile and awareness of the privacy principles. In addition, the go/privacy intranet page enables the sharing of good practice through a central resource of privacy related material.
- The newly introduced Privacy Design Document (PDD) clearly sets out all data collated by a project and the PDD process allows for oversight and review of projects by cross functional teams drawn from engineering, legal and product. This process is owned by the Privacy Engineering Team and defines the responsibility of project engineers to submit and maintain a PDD for all projects.
- The PDD process has clear, documented prioritisation guidelines for escalating projects for further review and a system for ensuring that identified privacy concerns are addressed. The PDD process has also

introduced the use of code audits for projects which are identified as carrying increased privacy risk, for example location based projects.

## 5.2 Areas for Improvement.

- Alongside the PDD process, Google have implemented new initiatives such as Privacy Stories. As such Google now have a number of privacy processes and initiatives at different stages of maturity as well as a number of functions delivering separate privacy related training. The ownership and delivery of Google's privacy processes and training should be reviewed to ensure they have a coordinated and targeted approach and to identify any possible synergies to reduce the risk of inconsistencies and gaps.
- While enhanced core training for engineers and other important groups has been developed and piloted, this needs to be fully rolled out as planned across Google. Further modules should be developed in relation to specific engineering disciplines and these should take account of the outcomes of the PDD and Privacy Story processes.
- The Google Code of Conduct and the related training should be updated to include specific reference to Google's five privacy principles.
- The tracking of core training participation and attendance should be improved to ensure all relevant employees receive the appropriate privacy training.
- While there are benefits in a business wide, consistent PDD process, Google should expand and iterate the PDD process to cover a range of different types of products to ensure all privacy matters for products are captured.
- All projects with a Tech Lead need to have a PDD and workflow tools should continue to be developed to track PDD submissions, maintenance and review to ensure they are completed for all relevant projects and are being kept up to date.
- Google should ensure random checks are undertaken across all PDDs to ensure completeness and accuracy, including undertaking Privacy Code Audits on a spot check basis. The results should be recorded and followed up where appropriate.
- All existing products need to have a Privacy Story, including those which are well established. Google should use the information gained through the completion of PDDs and Privacy Stories to proactively provide users with information about privacy feature of products.

---

## **6. Audit Approach**

- 6.1 The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of relevant documentation, an on-site visit including interviews with selected staff, and an inspection of selected records.
- 6.2 The audit field work was undertaken at Google Inc, London, on the 19<sup>th</sup>-20<sup>th</sup> July 2011.

*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 risk management, governance and internal control arrangements in place rests with the management of Google Inc.*

*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.*

## Appendix 1 - Schedule 1, Audit Scope

**Objective:** Review of Google Inc.'s ("Google") enhanced privacy processes in response to Street View Wi-Fi collections, as announced by Google in a Blogpost on October 22, 2010 ("Processes"). Such Processes are reflected in the form of an undertaking at points 1 to 5 above.

**Framework:** Google will conduct an internal assessment and provide a confidential written report ("Privacy Report") to the Commissioner. This Privacy Report will analyze Google's implementation of the privacy process changes it outlined on October 22, 2010 as it applies to Google's UK operations. The Information Commissioner's Office may then validate the Privacy Report's accuracy and findings via an in-person meeting to review the Privacy Report at Google's U.S. headquarters or at the offices of Google's UK subsidiary. Google shall provide the Privacy Report to the Commissioner before such meeting.

**Scope of audit:** Google's Privacy Report will cover the following areas:

### 1. Internal Privacy Structure

As announced on October 22, 2010, Google has appointed Dr. Alma Whitten as Director of Privacy across Engineering and Product Management. Google will provide the Commissioner's Office with details regarding the development of Dr. Whitten's Privacy Team, other privacy focused teams, and their initiatives within Google. It will also analyze cross-functional privacy efforts across engineering, product management, compliance and internal audit functions.

### 2. Privacy Training & Awareness

The Privacy Report will provide an overview of Google's revamped privacy training and awareness efforts. It will summarize the substance of training and awareness initiatives provided to Google employees, engineers, product managers, as well as employees in the legal, sales, and human resources departments. Furthermore, the report will identify the owners of these training modules.

### 3. Privacy Reviews

An assessment of Google's privacy reviews for products will be conducted. Among other things, the report will discuss the implementation of Privacy Design Documents, and analyze related processes including code audits undertaken against these documents. The Privacy Report will also provide the Commissioner's Office with an overview of reviews such as our annual Safe Harbor certification, and other processes in place to assure compliance with UK laws and privacy principles.