

Public Service Reform Directorate
Efficiency and Transformational Government Division
Area 3 H South
Victoria Quay
EDINBURGH
EH6 6QQ



T: 0131-244 3173
E: PrivacyPrinciples2009@scotland.gsi.gov.uk



31 August 2009

Dear Consultee

PRIVACY AND PUBLIC CONFIDENCE IN SCOTTISH PUBLIC SERVICES: DRAFT IDENTITY MANAGEMENT AND PRIVACY PRINCIPLES

I am writing to seek your views on the attached consultation document which contains draft Identity Management and Privacy Principles.

Background

People are often asked by public service organisations to prove that they are who they say they are - either to prevent fraud or to show that they are entitled to receive a particular service or benefit. They want to know that public authorities and other organisations respect their privacy and recognise the harm which may be done if personal information is collected or held unnecessarily, or lost or misused.

These draft Principles have been developed by the Scottish Government to help ensure that respect for privacy is central to the way public services prove identity or entitlement and to help public service organisations comply with data protection and human rights legislation.

These draft Principles will enable public organisations to build on these requirements and to achieve good practice.

The purpose of this consultation is to seek your views on these draft Principles.

The consultation period starts on 31 August 2009 and will run for 12 weeks. The deadline for responses is **Monday 23 November 2009**.

Following the end of the consultation period and subject to the views of respondents, the draft Principles will be finalised and disseminated.

Victoria Quay, Edinburgh EH6 6QQ
www.scotland.gov.uk



Consultation paper and consultation list

The consultation paper and questions are attached, along with a list of consultees. We have tried to cover all relevant interests but if you feel another party would benefit from seeing this consultation, please forward a link to this consultation or pass on a copy.

This consultation and all other Scottish Government consultation exercises can be viewed online on the consultation web pages of the Scottish Government website at <http://www.scotland.gov.uk/consultations>.

Responding to this consultation paper

I invite online, written or email responses to this consultation paper by **Monday 23 November 2009**.

Please use the online form at www.scotland.gov.uk/privacyprinciples2009

Or send your response to:

PrivacyPrinciples2009@scotland.gsi.gov.uk or:

Caroline Irving
Privacy Principles Consultation
Scottish Government
3-H South
Victoria Quay
Edinburgh
EH6 6QQ

Please include a completed Respondent Information Form (see "Handling your Response" below).

Handling your response

We need to know how you wish your response to be handled and, in particular, whether you are happy for your response to be made public. Please complete and return the attached **Respondent Information Form** at the end of this letter (or if emailing you can use the interactive Word Document found at www.scotland.gov.uk/privacyprinciples2009. The Online Response Form includes the Respondent Information Form): doing so will ensure that we will treat your response appropriately. If you ask for your response not to be published we will regard it as confidential and we will handle it accordingly.

All respondents should be aware that the Scottish Government is subject to the provisions of the Freedom of Information (Scotland) Act 2002 and would therefore have to consider any request made under the Act for information relating to responses to this consultation exercise.

Where respondents have given permission for their response to be made public, copies will be made available to the public in the Scottish Government library and on the Scottish Government web pages. Where agreement to publish has been given, we will check all responses for any potentially defamatory material before logging them in the library or placing them on the website.

Next steps in the process

Where respondents have given permission for their response to be made public and after we have checked that they contain no potentially defamatory material, responses will be made available to the public in the Scottish Government Library (see the attached Respondent Information Form). These will be made available to the public in the Scottish Government Library by 21 December and on the [Scottish Government consultation](#) web pages by early January. You can make arrangements to view responses by contacting the SG Library on 0131 244 4552. Responses can be copied and sent to you but a charge may be made for this service.

What happens next?

Following the closing date all responses will be analysed and considered along with any other evidence to help finalise the draft Principles. We aim to issue a report on this consultation process during February 2010 with a view to publishing the final Principles for use by public service delivery organisations in Scotland by early spring 2010.

Comments and complaints

If you have any comments about how this consultation exercise has been conducted, please send them to me at the address above.

Yours sincerely

CAROLINE IRVING
Policy Manager

Privacy and Public Confidence in Scottish Public Services: Draft Identity Management and Privacy Principles

Contents

Ministerial Foreword	5
Introduction.....	6
1. Proving Identity or Entitlement.....	7
2. Governance and Accountability	8
3. Risk Management	9
4. Data and Data Sharing	10
5. Education and Engagement	11
Glossary	12

Ministerial Foreword

Respect for privacy should be central to public services managing people's identity information. I want the public to be able to trust and have confidence in Scottish public services that are not only effective and secure but also privacy-friendly.

Existing data protection and human rights legislation govern personal information management by providing privacy protection. These *draft Identity Management and Privacy Principles* have been developed for Scottish Ministers by an expert group¹ to help public service organisations comply with such legislation and support good practice. I now look forward to hearing your views on this consultation.

These guiding Principles are aimed at both policy makers and practitioners in public service organisations concerned with systems for proving identity or entitlement to public services.

In addition to privacy legislation and these high level Principles, policy makers and practitioners already have access to practical guidance, such as from the Information Commissioner's Office and technological solutions, such as Privacy Enhancing Technologies. Together, I believe they will present a major step forward in achieving privacy-friendly Scottish public services.

John Swinney
August 2009

¹ The expert group's members were: Ken Macdonald, Assistant Commissioner for Scotland, Information Commissioner's Office: Rosemary Jay, Partner at Pinsent Masons LLP: Jerry Fishenden, Lead Technology Advisor, Microsoft UK: Gus Hosein, from Privacy International: Charles Raab, Professor Emeritus and Honorary Fellow at University of Edinburgh: Alan Kirkwood Chair of SociTM Scotland: and Duncan Macniven, Registrar General for Scotland.

Introduction

People are often asked by public service organisations to prove that they are who they say they are - either to prevent fraud or to show that they are entitled to receive a particular service or benefit, for example, free bus travel.

People want to know that public authorities and other organisations respect their privacy and recognise the harm which may be done if personal information is collected or held unnecessarily, or lost or misused. These draft Principles have therefore been developed by the Scottish Government for policy makers and practitioners in public service organisation, to help ensure that respect for privacy is central to the way public services prove identity or entitlement. They will also help public service organisations to comply with data protection and human rights legislation. That legislation governs personal information management by providing privacy protection. These draft Principles will enable public organisations to build on these requirements and to achieve best practice.

The draft Principles have been developed to give guidance on identity management² and privacy to public service organisations and they apply to all new systems and any systems which are being redesigned or redeveloped which involve identity management.

The draft Principles which follow cover the following five sub topics:

1. Proving Identity and Entitlement
2. Governance and Accountability
3. Risk Management
4. Data and Data Sharing
5. Education and Engagement.

A Glossary is provided at the end.

What happens next

Following the public consultation, the final Principles will be published. The Principles will be reviewed annually to ensure that they remain up-to-date, relevant and useful. Updated versions will be issued when necessary.

² The enrolment and subsequent verification that gives individuals trusted means to prove who they are to others and / or entitlement to a service or benefit.

1. Proving Identity or Entitlement

Only identify when necessary

1.1 People should not be asked to prove who they are unless it is necessary. A person making a general enquiry about a service should not need to provide any identifying information.

Ask for as little information as possible

1.2 People should be provided with an effective way of proving their identity or demonstrating entitlement to a service, based on the minimum level of information necessary. Therefore, public service organisations must only ask for the information they need in order to establish entitlement to a service. For example, if all that is needed is to know whether a person is retired, or over 18 years old, then no more information should be asked for.

Identify only once

1.3 For services which are used frequently and for which identification is needed, public service organisations should give people a simple way to register once. Thereafter, unless there is a statutory requirement to prove identity, in many cases a person should be able to access the service using a token, such as a bus pass or library card that proves their entitlement without revealing unnecessary personal information. In other circumstances, a user name and a password or elements of a password may be required.

Identify your organisation too

1.4 Public service organisations must provide ways for people to confirm that anyone claiming to represent the organisation, whether in person, by telephone, in writing or online, does in fact do so.

Ensure that authentication is effective and sufficiently reliable

1.5 The authentication methods³ selected should take into account convenience to the individual and respect for the individual's privacy. Organisations should also ensure that the means of checking identity are sufficiently reliable. In particular, they should take account of the extent to which the mechanism generates false rejections and acceptances and the consequences of these, including potential prevention of access to services or benefits, or failure to prevent fraud. Public service organisations must not rely, as the sole means of authentication, on personal information such as mother's maiden name which is quite easily found out, as this may increase the risks of fraud.

Avoid discrimination

1.6 Organisations must take steps to ensure that people are not discriminated against unfairly (for example, on grounds of disability, age or ethnicity) or socially excluded as a result of the approach to identification or authentication.

Offer choice

1.7 As far as possible, people should be offered alternative ways to prove identity and / or entitlement.

³ The method(s) used to prove ownership of identity and / or to demonstrate entitlement to services.

2. Governance and Accountability

Adopt privacy and security policies & procedures

2.1 Public service organisations using personal information on behalf of public authorities should adopt clear, coherent and verifiable policies on privacy and security. This should include policies which will aim to ensure that:

- a) a Privacy Impact Assessment (PIA) or proportionate equivalent is conducted and published prior to the implementation of a project which involves the collection of personal information;
- b) only the minimum amount of personal information needed for a specific purpose is collected, used or kept; that appropriate consent is obtained where necessary and that systems used for personal data comply with legal and regulatory requirements;
- c) the best available techniques are used to ensure the security of personal information throughout its lifecycle including while they are sharing information and through to archiving it; in particular, the organisation must abide by government standards for the use of encryption for the storage and transmission of this information; and that staff follow relevant guidance issued by the Information Commissioner's Office (ICO)⁴ and implement recommendations arising from the 2008 Scottish Government *Data Handling in Government* report;⁵
- d) personal data is only retained as long as is necessary and subsequently destroyed in a secure manner.

2.2 Public service organisations must ensure that the policies and standards are supported by appropriate procedures, control the use of authorisation and identity management systems and can deal effectively with compliance failures and breaches.

2.3 Responsibility and accountability for privacy should be assigned to a named senior management officer who reports to the Board or equivalent.

Audit

2.4 Public service organisations must be able to demonstrate that personal information can only be accessed by staff who need access to it. Organisations must ensure that they keep records of access to personal information, that there are alerts which prevent or identify inappropriate access and that access logs and alerts are reviewed regularly by line managers.

2.5 If a person discloses personal information to prove identity or entitlement, public service organisations should not take or retain copies of that information (such

⁴ The ICO is the UK's independent authority set up to promote access to official information and to protect personal information by promoting good practice, ruling on eligible complaints, providing information to individuals and organisations and taking appropriate action when the law is broken.

⁵ <http://www.scotland.gov.uk/Resource/Doc/229747/0062215.pdf>

as scans of driving licences or utility bills) unless this is essential for legal or audit purposes. In such cases, it would not normally be necessary to retain a copy of the full document; only the minimum amount of information to fulfil the legal / audit purposes would be required.

Accompany personal information with metadata

2.6 Where personal information is collected or stored, all reasonable steps should be taken to make sure that it is accompanied by information about the source, consent notice, permitted uses, retention period and other relevant metadata (i.e. data about data). Where information is shared within or beyond the public authority, it should be accompanied by this metadata to facilitate proper management of the information at its destination.

Facilitate oversight and reporting

2.7 The Scottish Government should work with the ICO to facilitate spot checks and the use of the ICO's forthcoming inspection powers and should co-operate with existing oversight organisations to include privacy issues in their inspections and reporting.

Apply Principles to contracts

2.8 Where public services are provided by non public sector organisations, organisations must acknowledge their duties in respect of personal information.⁶ In particular, where a public body has a contract with the private sector or the third sector, the contractor must be contractually bound to adhere to best practice as outlined in these Principles and other guidance. Public service organisations should ensure by contract that such organisations are required to permit the ICO to undertake spot checks on the processing of personal data being carried out in relation to the delivery of public services.

Parliamentary scrutiny of privacy impacts by lead committees

2.9 Where new primary or subordinate legislation is proposed, consideration should be given as to whether privacy issues will arise. If so, an appropriate Privacy Impact Assessment should be undertaken and a summary of impacts should be submitted for consideration by the lead committee in the Scottish Parliament.

3. Risk Management

Carrying out Privacy Impact Assessments (PIAs)

3.1 Public service organisations must carry out an appropriate level of PIA for any new initiative that enables access to services using IT and involves the collection, storage or use of personal information. Public service organisations must also carry out an appropriate level of a PIA if they are changing existing systems in ways which involve collection, storage or use of personal information.

3.2 Public service organisations should seek early involvement, at the policy development stage, of the ICO in Scotland.

⁶ See Section 1(4) of the Data Protection Act 1998 which stipulates that data controllers cannot divest themselves of their legal duties to contractors.

3.3 Public service organisations must make PIA documents publicly available, with easy access, before a new initiative is implemented.

Auditing existing initiatives

3.4 Public service organisations should consider privacy and data protection audits for existing initiatives.⁷

4. Data and Data Sharing

Acquiring and holding personal information

4.1 Public service organisations must minimise the personal information they hold, only acquire personal information for which they have a defined and specific need and ensure that such personal information is held only as long as is strictly necessary for the purposes for which it has been provided.

Avoid creating centralised databases of personal information

4.2 Organisations should seek to avoid creating large centralised databases of people's personal information. People's personal data should not be acquired and aggregated in a single place but maintained in separate data stores relevant to their specific business purpose. Organisations or their employees can still draw together personal information held in more than one place, if there is a business need to do so. That presents a lower risk than aggregating and storing all the personal information in a single place.

Storing personal and transactional data separately

4.3 Public service organisations must as far as possible store information about people's access to services separately from their personal data, to minimise the risk of data loss and to ensure that even if one set of information is accessed improperly, this does not allow access to a wider range of information about individuals. This may be achieved through the avoidance of centralised databases (see 4.2 above).

Controlling access

4.4 Public service organisations should ensure that personal data is held securely (see 2.1c above), that their employees only have access to the minimum personal information they need and that audit records exist of all accesses to, changes to and uses of that data.

Storing identifying information

4.5 Public service organisations must consider whether identifying information needs to be stored in a database at all. In some cases, it might be preferable for people to hold and manage their own identifying information which can be accessed by the public service organisation when it is needed. This could be achieved, for

⁷ (ICO, 2009, PIA Handbook:) "An audit is undertaken on a project that has already been implemented. An audit is valuable in that it either confirms that privacy undertakings and/ or privacy law are being complied with, or highlights problems that need to be addressed. To the extent that it uncovers problems, however, they are likely to be expensive to address and may disturb the conduct of the organisation's business. A PIA aims to prevent problems arising, and hence avoid subsequent expense and disruption."

example, by the information being held on a smartcard and accessed when required through a card reader.

Linking information between systems

4.6 Public service organisations should not share personal information unless it is strictly necessary. If a public service organisation needs to link personal information from different systems and databases, it should avoid *sharing* persistent identifiers; other mechanisms, such as matching, should be considered. If a public service organisation believes that persistent identifiers should be shared, it must publicly explain why.

5. Education and Engagement

Raise public awareness and understanding

5.1 The Scottish Government should work with public service organisations and others to raise the public's awareness and understanding about the issues covered in these Principles.

Educate people about identity management and privacy issues

5.2 Public service organisations must ensure that staff or contractors who handle personal data on their behalf have and maintain, a good working knowledge and understanding of identity management and privacy.

5.3 Public service organisations must take steps to ensure that their customers have enough information to make informed decisions about identity management and privacy.⁸

5.4 Public service organisations should remind people (both employees and the public) about the importance of protecting their personal data, including not disclosing their passwords or PIN numbers and not sharing their means of identification with others.

Inform and consult the public

5.5 If a public service organisation is planning or developing a system which involves personal information, it must inform and consult the public and particularly individual users (this is likely to be part of the PIA process). Where children are involved, it will be important to ensure that parents / guardians are also appropriately consulted.⁹ Methods of consultation and involvement must match the needs of the audience.¹⁰

Justify and communicate choices

5.6 Public service organisations must work to build public confidence and trust in their systems and practices. They must explain and communicate why information is

⁸ The ICO published a [Code of Practice on Privacy Notices](#) in June 2009.

⁹ Children aged 12 and above are presumed mature enough to exercise their rights under the Data Protection Act 1998.

¹⁰ Helpful pointers to best practice and innovative methods of public engagement and consultation are available from groups such as Involve (www.involve.org.uk), the International Association for Public Participation (www.iap2.org) and the Consultation Institute (www.consultationinstitute.org).

needed, how it is handled and where and why it is shared. They should also provide a clear explanation of the expected benefits and pitfalls of their authentication mechanisms.

Provide easy access to own data

5.7 Public service organisations should provide simple, quick and effective means for individuals to access information held about them. This might include secure electronic access to check and correct the data that is held on them (any such provision would need to be audited and regulated so that the security and accuracy of data is not compromised).

Duty to repair or redress

5.8 Where an individual demonstrates emotional or material harm arising from incorrect or misused personal information held about them, organisations should assume a duty to repair that information and redress the harm as appropriate.

Glossary

Authentication: The process of proving ownership of identity and / or demonstrating entitlement to services.

Authentication mechanism(s): The method(s) used to prove ownership of identity and / or to demonstrate entitlement to services. These include:

- **User name, password and Personal Identification Numbers (PINs):** These are typically a non-confidential name and a confidential password or number which are shared between a person and a system which may be used alone or together to allow specified access rights to the system.
- **Known Facts:** Information stored by a service provider or organisation to authenticate an individual seeking access to a service, such as current address.
- **Shared Secrets:** A piece of pre-agreed information such as a password or phrase or Questions and Answers, that is only known to the parties involved in a secure communication, such as between an individual and a service provider.
- **Smartcards:** A card containing a microchip which is capable of storing information, such as entitlements to free bus travel.

Biometrics: Measurable biological or behavioural characteristics that can be used for automated recognition. Biological biometrics include fingerprint; face; iris, hand geometry and palm vein patterns. DNA can be regarded a biometric technology once **data matching** (i.e. comparing and / or linking information from different sources) can be performed reliably using automated methods. Behavioural biometrics include voice and signature. Biometrics can also refer to the process of using automated methods for identifying a person by their biological or behavioural characteristics.

Encryption: The process of converting information into a code, by using a sequence of instructions (an *algorithm*) to make the information unreadable to anyone except those possessing special knowledge (usually referred to as a *key*).

Identifier: Frequently a sequence of characters and / or numbers that is used and / or assigned by an organisation to a person to identify *uniquely* the person for the purposes of the organisation's systems and operations. A Persistent Identifier is an identifier which will remain the same regardless of where the identifier is located, for example, one which is used in several independent databases.

Identity Management: The enrolment and subsequent verification (i.e. the decision made as a result of authentication) that gives individuals trusted means to prove who they are to others and / or are entitled to a service or benefit. An Identity **Management System** is the infrastructure which specifies the ownership, use and storage of information involved in managing identity.

Privacy Impact Assessment (PIA): This is a risk management technique for projects that involve personal information or intrusive technologies, conducted at an early stage of a new project or when a considerable change to a project is planned, to identify and address privacy issues. A PIA helps to explain how an organisation considered privacy in the design and implementation of a system and communicates this to users and people whose information is used. The Information Commissioner's Office (ICO) produced a [Handbook](#)¹¹ to help organisations decide whether a PIA is appropriate and to help them carry out a PIA.

¹¹ http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf

QUESTIONS

Note

We welcome comments on any of the draft Principles and the Glossary in addition to specific consultation questions set out below.

If you are responding to any of the questions set out below, we would be grateful if, for whichever method you use, you could clearly indicate in your response which questions or parts (e.g. Principle number) of the consultation paper you are responding to as this will aid our analysis of the responses received.

Question 1

Do you think it is clear what it meant by “best available” techniques in draft Principle 2.1 c?

Yes

No - Please use the space below to provide details as it is important for us to understand why not.

Question 2

Do you think the scenario described in the first sentence of draft Principle 2.4 works in all settings including, for example, clinical contexts?

Yes

No - Please use the space below to provide details as it is important for us to understand why not.

Question 3

Do you think draft Principle 2.9 is an appropriate way of safeguarding citizen’s privacy?

Yes

No - Please use the space below to provide details as it is important for us to understand why not.

Question 4

Draft Principle 4.6 refers to persistent identifiers being shared outside their existing context or governance boundaries - is the existing wording clear enough?

Yes

No - Please use the space below to provide details as it is important for us to understand why not.

Question 5

Do you have specific concerns that draft Principle 5.7 will be complex and / or expensive to implement as a result of data being stored in separate databases (draft Principle 4.2)?

Yes - Please use the space below to give details about your specific concerns.

No

Question 6

Do you think it would be useful to provide examples of practical approaches to the Principles?

Yes - Please use the space below to specify, for example, for which Principles you would like examples or other additional information.

No

Question 7

Do you have other comments on any of the draft Principles or the Glossary (in addition to specific consultation questions above)?

Yes - Please provide your comments in the space below.

No

CONSULTATION LIST

A number of individuals
ACPOS
Clerks of the Committees of the Scottish Parliament
CoSLA
Department Committee Liaison Officer
Disclosure Scotland
Equality and Human Rights Commission
General Register Office for Scotland
Human Rights Commissioner
Improvement Service
Learning & Teaching Scotland
Legal Deposit Libraries
Local Authority (32) - Chief Executives
NHS 24
NHS Boards (14) - Chief Executives
NHS Quality Improvement Scotland
Scottish Council for Voluntary Organisations
Scottish Information Commissioner
Scottish MEPs
Scottish Public Services Ombudsman
Social Work Inspection Agency
SPICe, Scottish Parliament
Student Awards Agency for Scotland
Transport Scotland



RESPONDENT INFORMATION FORM

Please Note That This Form **Must** Be Returned With Your Response To Ensure That We Handle Your Response Appropriately

1. Name/Organisation

Organisation Name

Title Mr Ms Mrs Miss Dr Please tick as appropriate

Surname

Forename

2. Postal Address

Postcode	Phone	Email

3. Permissions

I am responding as...

Individual <input type="checkbox"/>	/	Group/Organisation <input type="checkbox"/>
<i>Please tick as appropriate</i>		

(a) Do you agree to your response being made available to the public (in Scottish Government library and/or on the Scottish Government web site)?

Please tick as appropriate Yes

(b) Where confidentiality is not requested, we will make your responses available to the public on the following basis

Please tick ONE of the following boxes

Yes, make my response, name and address all available

or

Yes, make my response available, but not my name and address

or

Yes, make my response and name available, but not my address

(c) The name and address of your organisation **will be** made available to the public (in the Scottish Government library and/or on the Scottish Government web site).

Are you content for your **response** to be made available?

Please tick as appropriate

(d) We will share your response internally with other Scottish Government policy teams who may be addressing the issues you discuss. They may wish to contact you again in the future, but we require your permission to do so. Are you content for Scottish Government to contact you again in relation to this consultation exercise?

Please tick as appropriate