Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

9 April 2015

Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Secretary,

Re: Migration Amendment (Strengthening Biometrics Integrity) Bill 2015

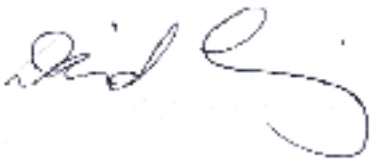
The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached.

The Australian Privacy Foundations thanks the Committee for the opportunity to make a submission to this inquiry. The Bill poses substantial privacy concerns that we urge the Committee to consider.

Please find attached the APF's Submission to this Inquiry.

Thank you for your consideration.

Yours sincerely



Kat Lane, Vice-Chair
0447 620 694
Kat.Lane@privacy.org.au

(Dr) David Lindsay, Vice-Chair
(03) 9905 5547
David.Lindsay@privacy.org.au

David Vaile, Vice-Chair
0414 731 249
David.Vaile@privacy.org.au

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby and Elizabeth Evatt, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-) http://www.privacy.org.au/Campaigns/Media/

Australian Privacy Foundation

Submission re Migration Amendment (Strengthening Biometrics Integrity) Bill 2015

9 April 2015

APF's Standing as an Interested Party

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached.

The APF has been a regular contributor to inquiries and reviews concerning the use of biometrics and national security regimes for more than 20 years. Our submissions can be found at: http://www.privacy.org.au/Papers/.

In particular, we draw attention to recent submissions to the Parliamentary Joint Committee on Intelligence & Security (PJCIS) relating the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014* (October 2014) and Potential Reforms of National Security Legislation (August 2012). The APF has had a Policy Statement in place in relation to Biometrics since 2008. A copy is attached, and forms part of this Submission.

Overview and Objectives of the Bill

The Migration Amendment (Strengthening Biometrics Integrity) Bill 2015 expands the type of biometric data, the number of agencies with the power to collect biometric data, and authorizes collection on both Australian citizens and non-citizens. The location of collection also expands, introducing collection at ports of entry (airports and seaports) as well as expanding biometric collection possibilities 'inland' through the use of mobile hand-held devices.

Justification by the government for the broadened mandate in biometric collection is rooted in prevention of terrorism, identity fraud, and the mitigation of human trafficking including children. The collection and storage of biometric identifiers are expected to disclose criminal histories and deny the possibility future criminal acts.

However, while the context of the Bill is national security concerns, biometric screening of entire populations has not been found to be an effective response to the prevention of terrorism (see Appendix 1). One does not need to assume a false identity to commit a criminal act. In light of concerns over the efficacy of biometric systems (on technical and operational grounds), the collection of biometric identifiers across entire populations presents serious privacy concerns.

There is currently no evidence of a Privacy Impact Assessment (PIA) or advanced consultation with the Office of the Australian Information Commissioner (OAIC) or expert civil society groups. Furthermore, any expansions in the scope of the regime under the current text of the Bill is possible without further parliamentary oversight and transparency.

The following submission reviews the policy intentions of the creation of the new section 257A in the Migration Act 1958 (Cth). This amendment replaces eight existing provisions to authorize a single broad power to collect biometric 'personal identifiers'. The submission highlights a number of privacy concerns that the APF has identified with the program. Given these issues, the APF strongly recommends that all biometric programs be currently subject to moratorium. The APF has had a Policy Statement in place in relation to Biometrics since 2008. A copy is attached, and forms part of this Submission.

Requirement to Consult on Privacy Concerns

The Explanatory Memorandum (EM) and the Bill currently provide no indication of what safeguards would be in place to protect privacy and ensure the security of biometric information.

While the Statement of Compatibility associated with the Bill notes a "negative impact on privacy" in light of the "widespread collection of personal identifiers", there is no current evidence that indicates a PIA and/or consultation with the OAIC has been undertaken. Nor has consultation with civil society groups and associated experts occurred beyond government consult. The APF is concerned that the Bill is being advanced without previously having undertaken the PIA and consultations as part of the development process.

In 2014, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) reviewed the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014 and proposed amendments to include collection of biometric identifiers were recommended. During that process, the PJCIS insisted (in Recommendation 36) that:

> "…the Government consult with the Privacy Commissioner and conduct a privacy impact statement prior to proposing any future legislative amendments which would authorize the collection of additional biometric data such as fingerprints and iris scans."

One key purpose of a PIA is to identify whether a less privacy intrusive measure can be taken that will provide similar outcomes based on the objectives of the program. Evidence that the widespread collection of biometric identifiers across the whole of the population might not always be proportionate, particularly in the context of future possibilities for mission-creep on technological, legislative, and regulatory fronts. The APF is concerned that the Bill is being advanced without previously having undertaken the PIA and consultations as part of the development process. A PIA would also consider very important issues associated with upholding the integrity and accuracy of stored information. The APF strongly recommends that a full PIA process and additional consultations with non-governmental organisations be undertaken immediately and prior to any further legislative developments.

Considering Children and Incapable Persons

The APF also raises a number of privacy concerns under the new section 257A, which authorizes the collection of 'personal identifiers' from minors and incapable persons without the consent or presence of a guardian or independent person.

While the EM states that the policy intent is to collect from a small number of minors in circumscribed circumstances (including offshore cases to protect minors from human trafficking), in principle, the Bill is currently written to extend to all Australian and non-Australian children and incapable persons.

Consistent with its longstanding positions on such matters, the APF strongly recommends that individuals that are subject to surveillance and collection of their personal information be adequately informed, in clear terms, the reasons for the collection; whether and under what conditions their personal information will be disclosed to third parties; and to what extent these surveillance measures will affect their privacy.

Information Security and Data Management Concerns

The costs of a data breach are extraordinarily high concerning privacy breaches associated with biometric identifiers. Unlike other documents that can potentially be replaced or changed (such as a passport, credit card, or tax file number) a data/privacy breach that includes biometric identifiers means that when a breach occurs the personal identifiers of Australian and non-Australians will be permanently misplaced.

There is serious cause for concern in the context of routine data breaches in Australian government. In the past year, the Immigration Department alone has encountered a number of privacy breaches. One notable example involved a breach of the personal information of approximately 10,000 asylum seekers that were inadvertently posted on the agency's website.[1] The APF policy on Data Breach Notification is attached to this submission.

1– Immigration slammed for privacy breach which saw asylum seeker records released, New Matilda, 12 November 2014 https://newmatilda.com/2014/11/12/immigration-slammed-privacy-breach-which-saw-asylum-seeker-records-released

The APF believes it is essential that any data management system be established in relation to strict system-wide information security protections. Architectural developments that impose rigorous data security mechanisms during transmission and storage are essential to prevent, theft, intrusion, and interception. While data security at the architectural level is paramount, the APF notes further concerns that proper measures be taken to protect against possible breaches within an organization. Strict audit logs concerning any access to biometric data is a bare minimum requirement to detect, deter, restrict, and potentially prevent compromise from internally situated actors.

Furthermore, the APF also notes that the use of the biometric program with mobile devices presents an additional information security concern that further jeopardizes the privacy of Australians and non-Australians alike. The use of mobile technology broadens the attack vector that can act as an additional beachhead for further access to networked infrastructure that houses biometric identifiers. The broadened networked architecture to include multiple agencies, devices, and officials with myriad access permissions also contributes to an unwieldy potential for inadvertent data breaches stemming from the technology and its use.

Mission-creep through Technical Developments and Inadequate Safeguards

The APF is concerned about a high likelihood for mission-creep associated with the current legislative proposals. Mission-creep occurs in two main ways—both through ongoing technological interfacing capabilities and in the absence of clearly entrenched safeguards in legislation. The current manifestation of the Bill raises concerns in terms of both technical and legislative aspects.
In terms of technical creep, biometric identifiers are increasingly able to interface with database technology that falls 'outside' of the traditional boundaries of a given biometric program. This raises additional privacy concerns that the creation of a biometric system for all Australians will find new and currently unexpected uses. Additional agencies might be interested in the capabilities as an identity token system to distribute organizational-specific entitlements in cases where biometrics are unfit for purpose. In recent times, biometric systems have been interfaced in policing and control environments with technologies that hitherto contained only video functionalities. The current legislation allows for the extension of biometric technologies into traditional policing environments, a development which given the serious intrusions posed for privacy deserves further scrutiny and debate.

In terms of policy and legislation creep, concerns persist that many of the 'safeguards' identified in the Bill and EM is situated as mere "policy intent". Given the lack of adequate protections in the legislation, the Bill is subject to mission-creep through ongoing policy expansions in the absence of adequate parliamentary oversight and public transparency.

The EM routinely insists that much of the important detail is left for policy. For instance, the EM states that restrictions to the collection of personal identifiers "will apply in policy only"; that the circumstances surrounding collection from minors and incapable persons "will be set out in policy"; that the offshore collection of personal identifiers "will be preserved in policy"; and that under paragraph 257A(5)(b) "there is no intent to implement anything in policy".

While the department does not intend to collect personal identifiers in all circumstances (such as fingerprints from non-citizens), the insistence that policy guidance will be given at a subsequent period excludes crucial detail from the legislation. As a result, insistence on "policy intent" through post hoc regulatory developments leaves open significant possibility for mission-creep associated with the Bill. This is especially the case when considered alongside the compounding effects of technological advancements.

A failure to provide clear legislative guidance also short-circuits informed discussion about the full privacy implications of the Bill. This furthers the possibility for the extended scope of collection and database interfacing through regulations, and as mentioned, in the absence of parliamentary oversight and public transparency.

Biometrics

Original Version of 5 April 2008 – Amended 15 October 2011

Summary

Technology providers are trying to sell biometrics schemes, and some organisations are buying them, without regard for the security and privacy of the people the schemes are being imposed upon. Now even school-children are being trained to submit to biometric measurement, and to accept physical intrusions and continual techno-surveillance as part of their lives.

This document expresses the APF's policy in relation to biometrics.

The APF's policy is that all biometric schemes must be the subject of a moratorium.

No new biometric schemes should be implemented until and unless comprehensive laws have been brought into effect to regulate them.

Each proposal must be demonstrated to be justified, must be subject to a Privacy Impact Assessment (PIA), including consultation with the affected people and their representatives and advocates, and must include appropriate safeguards. It will then be essential to review existing applications of biometrics, to ensure that they also measure up against the standards.

Background

A biometric is a measure of some physical or behavioural attribute of a person, which is intended to be unique, or at least sufficiently distinctive to assist in recognising who the person is.

Few if any biometrics are actually unique; but technology providers promote the myth that they are, and user organisations happily believe it. A great many biometric schemes have been invented, and many have failed and disappeared. Those currently in the market include fingerprints and iris scans (which under ideal conditions can produce some degree of reliability), hand geometry and voice scans (which under ideal conditions can be of some use in authenticating whether the person is who they purport to be), and so-called 'face recognition' technologies (which not only do not 'recognise faces', but are not even based on any attribute that could give rise to reliable distinctions between different people).

The most common form of biometric scheme involves a 'reference measure' being acquired for each person, together with an identifier such as their name, and stored somewhere. Subsequently, 'test-measures' can be compared against one particular reference measure, or against multiple reference measures.

For a great many reasons, the measurements are always inaccurate, and the matching is always 'fuzzy'; so results ought to be expressed as probabilities. But that is administratively inconvenient, so most biometric systems just determine a Yes/No result, based on some arbitrary threshold. The thresholds are set and adjusted pragmatically, in order to achieve a compromise between generating large numbers of 'false positives' (unjustified suspicions), on the one hand, and large numbers of 'false negatives' (failures to find what should have been matches), on the other.

Biometrics can be used for authentication. In this case, a test-measure is compared against a reference-measure for a particular person, and the decision is either that the person is accepted as being the right one, or rejected. Alternatively, biometrics can be used for identification, in which case the test-measure is compared against the reference-measures of large numbers of people. Authentication uses are error-prone, and in some cases such as 'face recognition', highly error-prone. Identification uses are highly error-prone, in some cases such as 'face recognition', hugely error-prone.

Biometrics have been implemented or proposed as a basis for forensic evidence in law enforcement and some civil cases, for identifying people at border-crossings, for controlling access to secure areas, for checking that a token (such as a passport or credit-card) is being presented by the person it was issued to, and for recording attendance (e.g. by people on parole, or on remand, but also for employees and even school-students).

APF POLICY re BIOMETRICS

1. Biometrics are Extraordinarily Privacy-Invasive

Biometrics invade the privacy of the physical person, because they require people to submit to measurement of some part of themselves. In many circumstances, people are required to degrade themselves, and submit to an act of power by a government agency or corporation, e.g. by presenting their face, eye, thumb, fingers or hand, or having body tissue or fluids extracted, in whatever manner the agency or corporation demands. This may conflict with personal beliefs and customs.

Biometrics invade the privacy of personal behaviour, because they are a key part of schemes that provide government agencies and corporations with power over the individual. That not only acts as a deterrent against specific undesirable behaviours, but also chills people's behaviour generally.

Biometrics invade the privacy of personal data, because biometric measurements produce highly sensitive personal data, and that data is then used, and in many cases stored and re-used, and is available for disclosure, e.g. by the Australian government to other governments, including U.S. immigration and national security agencies.

2. Biometrics are Highly Error-Prone and Unreliable

Biometric schemes try to impose rigid technology on soft human biology, and in enormously varying contexts. Among many other challenges, the nominally unique features are mostly three-dimensional, and vary over time, and hence it is simply not feasible to 'capture' a representation of the features into digital form in a consistent manner. The equipment has to cope with many different environmental conditions (such as the strength and angle of light, the humidity, the temperature, and the dust-content in the air). In addition, it is impossible to ensure that manual procedures are performed in standard, invariant ways by lowly-paid security staff.

The comparisons performed between measures ignore all of the subtleties and reach a decision that is more or less arbitrary. A proportion of people (somewhere between 2% and 5%, or between 400,000 and 1 million Australians) are 'outliers' whose measures will always be highly problematical (e.g. because their fingerprints are faint, or worn down). A further serious problem is that many people accept the imposition nervously, sullenly or uncooperatively, and some actively resist it and seek to subvert it – some of them with serious criminal intent, but others without it.

As a consequence of these problems, there are a great many sources of error. That in turn means that tolerance-ranges have to be set quite high. Errors that are 'false-negatives' mean that the system doesn't achieve its primary objective. False-positives, on the other hand, give rise to wrongful suspicions, create considerable anxiety for the people concerned, and deflect organisational focus and resources away from more effective security measures.

3. Biometrics are Highly Insecure

An individual or organisation that acquires a person's biometric can use it to commit identity fraud or outright identity theft, and to 'plant ' false evidence.

Biometric technologies are commonly able to be subverted in order to produce an 'artefact'. That enables a person to masquerade as someone else.

If a person's biometrics are compromised by someone else, they cannot be revoked. So the risk of 'biometric theft', which exists for everyone, lasts their whole life long. Hence, even if it makes sense to use biometrics for a very small number of really important purposes, it doesn't make sense to undermine such reliability as it has by using it for trivial applications.

4. Biometrics assist Identity Fraudsters and Thieves

Far from solving masquerade and identity theft, biometrics are actually part of the problem.

Biometrics technologies are opaque. Organisations don't understand them, but instead just assume that they work, without conducting continual tests to ensure that they are still functioning as they were intended to, and haven't been neutralised. So masquerades that subvert biometric technologies are highly unlikely to be detected.

Added to that, many biometric schemes involve reference-measures and test-measures being exposed in the data-gathering equipment, networks, intermediate storage and long-term storage. Particularly in long-term storage, the data is highly attractive, and it is impossible to prevent unauthorised uses, and 'function creep' to new purposes.

5. Biometrics Errors impose Serious Risks on Powerless People

Biometric schemes are imposed on people by powerful organisations. In most cases, no meaningful consent is involved. Yet the large numbers of failures to capture a usable measure and the many false-positives impact the affected individuals much more than they do the scheme's sponsor. Everyone who is subject to such errors suffers at least inconvenience and embarrassment. Much more serious problems are created for some people, who may be falsely accused of misbehaviour or

crime, unjustifiably detained by authorities, denied access to premises, or miss their flight.

Many biometric schemes effectively declare the individual to be guilty of something, and place the onus on the individual to prosecute their innocence. That is repugnant to traditional concepts of justice. In addition, very few people understand how biometric systems work, and hence very few people are capable of dealing with such situations. Even for those individuals who do understand the technology, it's very difficult to find anyone administering the system who is capable of carrying on a sensible conversation about the errors involved.

6. Biometrics demand Strong Justification

Because biometrics technologies are so highly privacy-invasive, it is totally inappropriate for organisations to implement schemes without conducting very careful design, demonstrating the effectiveness of the scheme and the ineffectiveness of alternatives, performing privacy impact assessments (PIAs), conducting consultation with affected parties and their representatives and advocates, and preparing cost-benefit analyses that show conclusively that the benefits justify the costs and disbenefits to all parties involved, including and especially the people it is imposed upon.

All schemes have substantial downsides that impact on the people involved. Most potential biometric schemes fail the test, and should not be implemented. Those that have already been implemented should be subjected to critical assessment. This would result in the abandonment of many existing schemes, and the refinement of other schemes in order to ensure that they include appropriate safeguards.

7. Biometrics do not Stop Terrorism

Proponents of biometrics spread misinformation, suggesting that biometric schemes are necessary to combat terrorism. This is simply false (e.g. Schneier 2001, Ackerman 2003, Clarke 2003). Terrorists are defined by the acts that they perform, not by their biometric. Virtually no terrorist act, ever, anywhere, would have been prevented had a biometrics scheme been in operation.

8. Biometrics grant Excessive Power to Corporations and States

Biometrics lays the foundation for corporations and the State to extend their power over individuals. People are cowed by the knowledge that their actions are monitored and recorded. That substantially reduces their capacity to exercise the rights and freedoms that they are supposed to have.

Organisations are in a position to deny access to services, premises and transport to people whose identity they are unable to authenticate, or who they (rightly or wrongly) deem to be a particular person whom they have (justifiably or otherwise) blacklisted. Widespread application of biometrics could see these powers extended to something so far only seen in sci-fi novels and films – outright identity denial.

9. A Highly Intrusive Error-Prone Technology requires Tight Regulation

The protections that are needed against the ravages of biometrics include:

- legal frameworks
- public justification for the measure
- the obligation to perform a PIA
- the obligation to conduct consultations with affected individuals and their representatives and advocates
- mechanisms to ensure the outcomes of the PIA are reflected in the scheme
- features built into technologies and products
- features designed into manual processes
- laws regulating biometric technologies
- laws regulating the practices of all organisations
- enforcement mechanisms
- sanctions for breaches
- enforcement actions

10. Biometrics are Subject to Almost No Regulation

There is an almost complete absence of such protections. There are virtually no statutory protections in place.

A Biometrics Privacy Code has been published, and accepted by the Privacy Commissioner. The Code was produced by the so-called 'Biometrics 'Institute'. But that organisation is merely an industry association, and one that grossly compromises accepted principles by including both sellers and buyers inside a single lobby-group. And the purpose of the 'Institute' in publishing its Code was to forestall formal regulation. The public interest has been relegated to the role of an onlooker.

That Code has been almost completely ignored by technology providers and user organisations, and has had no impact at all on industry practices. Self-regulation in this, as in so many other areas, has been an abject failure. Yet if organisations had complied with even that weak and ineffectual Code, some of the gross excesses that companies and government agencies seek to impose would have been prevented.

Created: 17 March 2008 - Last Amended: 15 October 2011 by Roger Clarke - Site Last Verified: 11 January 2009

Site Map - This document is at http://www.privacy.org.au/Papers/Biometrics-0804.html - Privacy Policy

APF Policy Statement on Data Breach Notification

A data breach occurs when personal data is exposed to an unauthorised person. It is a breach of trust by the organisation. It is commonly also a breach of the law. Unfortunately breaches of data protection laws are seldom subject to enforcement actions.

Data breaches occur remarkably frequently. Parliaments have failed to impose meaningful sanctions, and privacy oversight agencies have failed to exercise such powers and influence as they have to force organisations to ensure that appropriate security safeguards are in place.

In 2003, the Californian legislature responded to inadequacies in organisational practices by passing a Security Breach Notification Law. By 2006, 33 other US States had passed similar laws. Australian law reform has moved at glacial pace, and lags the US in this matter by a decade.

This document declares the APF's Policy on Data Breach Notification. It comprises the following sections:

Definitions

A **Data Breach** occurs where personal data held by an organisation has been subject to, or is reasonably likely to have been subject to, unauthorised access, disclosure, acquisition or loss.

A **Serious Data Breach** is a Data Breach that gives rise to a reasonable risk of harm to an individual.

A **Data Breach Notification** is a statement of the facts relating to a Data Breach.

The Purposes of Data Breach Notification

The purposes of Data Breach Notification are:

1. to inform the public, at a meaningful level of detail, about:
    - breaches
    - inadequacies in organisations' security safeguards
2. to inform individuals who have been affected by breaches, so that they can judge whether to:
    - take action to prevent or mitigate potential harm arising from the breach
    - seek compensation for harm caused
    - change their service-providers
3. to shame organisations that have seriously inadequate security safeguards into changing their ways
4. to encourage all organisations to implement adequate security safeguards

Data breach notification processes, guidelines and regulations need to be designed so as to achieve these purposes.

Organisations' Obligations in Relation to Data Security

1. All organisations must ensure that personal data is at all times subject to security safeguards commensurate with the sensitivity of the data. The APF has previously published a Policy Statement on Information Security

2. All organisations must take the steps appropriate in their particular circumstances to:
    - deter Data Breaches
    - prevent Data Breaches
    - detect Data Breaches
    - mitigate harm arising from Data Breaches; and
    - enable their investigation
3. All organisations must implement awareness, training and control measures to ensure appropriate practices by their staff
4. All organisations must conduct audits of security safeguards periodically, and when the circumstances warrant
5. All organisations must perform a Privacy Impact Assessment (PIA) when data systems are in the process of being created, and when such systems are being materially changed, in order to ensure that appropriate data protections are designed into their systems, and to demonstrate publicly that this is the case

---

Organisations' Obligations in Relation to Data Breach Notification

1. Conduct of an Investigation

Where grounds exist for suspecting that a Data Breach may have occurred, the organisation must conduct an investigation, in order to establish a sufficient understanding of the circumstances and the outcomes. The results of the investigation must be documented in a form that enables subsequent evaluation.

2. Submission of a Data Breach Notification

Where a Data Breach has occurred, or is reasonably likely to have occurred, the organisation must:

1. Submit a Data Breach Notification to the relevant oversight agency, in a manner consistent with the guidance issued by that oversight agency, as soon as practicable and without delay
2. Communicate sufficient information to affected categories of individual, the media, and/or representative and advocacy agencies, as appropriate to the circumstances

3. Form of a Data Breach Notification

A Data Breach Notification must include sufficient detail to enable the reader to achieve a proper understanding of the Data Breach, its causes, its scale, its consequences, mitigation measures, and the rights of individuals affected by it.

Details whose publication might result in harm or facilitate attacks on that or other organisations can be included within a separate Appendix whose distribution can be limited.

4. Additional Obligations in the Case of a Serious Data Breach

Where a Serious Data Breach has occurred, or is reasonably likely to have occurred, the organisation must, in addition:

1. Provide an explanation, apology and advice to each individual whose data is, or is reasonably likely to be, the subject of the Data Breach, as soon as feasible and without delay, but taking into account the possible need for a brief delay in the event that criminal investigation activities require a breathing-space
2. Publish an appropriate notice and explanation in a manner that facilitates discovery and access by people seeking the information
3. Where material harm has occurred, provide appropriate restitution
4. Inform the oversight agency of the actions taken

The Reponsibilities of the Oversight Agency

1. Publish guidance in relation to data security safeguards.
This must make clear that organisations have obligations to perform Security Risk Assessment, and to establish an Information Security Risk Management Plan whereby information security safeguards are implemented and maintained, commensurate with the sensitivity of the data

2. Publish guidance in relation to Data Breach Notifications

3. In relation to Data Breaches:

- Liaise with organisations that have suffered Data Breaches
- Facilitate the Submission of Data Breach Notifications
- Inform the Public
- Publish the Data Breach Notifications in a Public Register

4. In relation to Serious Data Breaches:

- Review the outcomes of the organisation's internal investigation
- Where doubt exists about the quality of the internal investigation, conduct its own independent investigation
- Publish the results of the review and/or investigation
- Add details of the investigation into the Public Register

5. Facilitate improvements in organisational practices relating to data security

6. Facilitate remedies for individuals who have suffered as a result of Data Breaches

---

Enforcement

All obligations in relation to Data Breach Notification must be subject to sanctions and enforcement.

The sanctions applied must reflect:

- the organisation's degree of culpability, including:
  - the extent to which the organisation had implemented safeguards commensurate with the sensitivity of the data
  - the extent to which the threat(s) and vulnerability/ies that gave rise to the Data Breach were well-known or novel
- the promptness and effectiveness with which the organisation reacted once grounds existed for suspecting that a Data Breach may have occurred
- mitigation measures adopted by the organisation once it was apparent that a Data Breach had occurred, or was reasonably likely to have occurred
- any avoidance activities, misinformation or delays by the organisation in responding to the Data Breach and in its interactions with the oversight agency
- the scale of the Data Breach
- the sensitivity of the data that was the subject of the Data Breach
- the measures undertaken by the organisation in order to address the risk of recurrence of Data Breaches (as distinct from the organisation's statements about what it intends to do)
- to the extent that financial penalties are applied, the size of the organisation

---