SYNOPSIS GROUP

Whitepaper: How data classification enables privacy compliance.

Date Created: 27th November 2019

Version Control:

Version	Description of Changes	Date	Author(s)
Draft	Creation of document	27/11/2019	Nardus Schroeder

Contents

How data classification enables privacy compliance.

Introduction

In this whitepaper, we'll explore:

- The new privacy and data protection legal environment
- The intersection between privacy law and information security practice u How data classification enables data protection u Protecting data, even when sharing data
- Simple ways to improve security culture across the enterprise.

Background

Around the world, new privacy and data protection laws are driving the need for significant operational and technological responses. The challenge of protecting personal data in particular is big news: with the commencement of the General Data Protection Regulation (GDPR) in May 2018, fines for failing to comply with privacy laws will reach up to €20 million, or 4% of a company's annual global turnover.[1]

At the same time, there is increasing pressure on both governments and corporates to release the value 'locked up' in their data holdings, so that data analytics can yield insights of public benefit. The promise of big data is that it can have a transformative impact on our way of life, offering opportunities to "grow our economy,

"Big data, fuelled largely by personal data about all of us, represent an asset class every bit as valuable as gold or oil." Boston Consulting Group

improve health and education, and make our nation safer and more energy efficient".[2] However being able to fully realise the value of big data requires organisations to establish "rules and processes around the use and management of personal data so that the risks are properly mitigated".[3]

Resolving these tensions requires a finely-tuned response, so that personal data and confidential data remain robustly protected, while the process of sharing appropriate data with authorised parties is simplified.

The Brave New World of Privacy and Data Protection

New privacy laws are driving a significant increase in emphasis on data protection, for organisations around the world. All eyes are currently on Europe, where the penalty regime in the GDPR is focussing the attention of the C-suite on what needs to be done, to ensure legal compliance and effective data protection. Even businesses based outside the EU will be impacted by the GDPR: no matter where an organisation is located, if it offers goods or services to, or monitors the online behaviour of, European residents, then it will become regulated under European privacy law from May 2018.

But it's not just in Europe that privacy laws are getting tougher. Increasingly, new-generation privacy and data protection laws require organisations to be proactive. This means that if you don't have an effective privacy compliance program, you can be found in breach of your data protection obligations even if you don't suffer a data breach. This requirement to be proactive, also known as the Accountability privacy principle, is a feature of the GDPR. It is also found in the APEC Privacy Framework,[4] as well as in Canadian and Australian privacy laws.[5]

There is also a strong focus on getting reactive strategies right. Although data breach notification requirements have been around in the United States for some years now, the GDPR ramps up the pressure, by setting a default 72-hour timeframe on notifying the relevant regulator.[6] However the requirement to notify data subjects of a personal data breach does not apply if the company had "appropriate technical and organizational measures" in place to protect the data.[7] Australia and New Zealand look set to follow, with new data breach notification laws expected in 2017.

Enforcement action in the USA is also ramping up, the latest case involving a failure to implement data loss prevention strategies or technologies, which resulted in a US$3.2M civil penalty following both loss and theft of thousands of children's medical records.[8]

The Intersection Between Privacy Law and Information

Security Practice

European privacy law uses the term "personal data", which means "any information relating to an identified or identifiable natural person". Under the GDPR, the scope of this concept has been clarified and expanded, to clearly include online identifiers, geolocation data, and pseudonymous data. In the United States, the phrase commonly used is "personally identifiable information", or 'PII', while in Australia, New Zealand and Canada, privacy laws refer to "personal information".

The commonality between all these different laws is that if any individual is identifiable from a set of data, then a particular set of legal obligations will be invoked. The actual obligations also differ between jurisdictions, but tend to cover similar ground:

- **Collection Minimisation:** limit the collection of personal data to only what is necessary
- **Use Limitation:** only use personal data for the purpose for which it was collected, unless authorised otherwise
- **Restrictions on Disclosure:** additional restrictions on disclosing personal data to third parties, particularly 'trans-border' disclosures
- **Data Quality:** ensure the accuracy of the personal data before using or disclosing it
- **Data Security:** protect personal data from loss, misuse and unauthorised disclosure
- **Access and correction rights:** people have the right to access the personal data held about them, and to seek its correction where warranted
- **Openness:** give people notice about each collection of their personal data, and allow people to understand how their personal data will be collected, used and disclosed
- **Accountability:** be proactive in ensuring compliance with privacy and data protection obligations, by developing a robust privacy compliance program

Some jurisdictions even set further restrictions on the collection, use or disclosure of certain sub-categories of personal data, such as health information, criminal records, information about ethnicity, religion or sexuality, biometric data, or unique identifiers such as driver licences or Social Security Numbers.

The Data Security principle underpins many of these obligations. If your information security practices are not up to scratch, the personal data you hold is more exposed to the risk of misuse or an unauthorised disclosure.
Principles-based privacy laws adopt a technology-neutral, risk-based approach, rather than a prescriptive approach. This allows the legal requirements to alter over time, to reflect industry best practice and available technologies at any given point. In this way, privacy legal obligations stay up-to-date, and will reflect the latest information security standards relevant to the organisation. For government agencies in particular, that may mean national or state/provincial requirements in relation to information security become a de facto part of the privacy law.

How Data Classification Enables Data Protection

'Information security' involves all measures used to protect information from compromise, loss of integrity, breach of confidentiality or unavailability. Historically businesses have focussed on protecting their most valuable data, which could reveal:

- Product development or marketing strategies
- Market-sensitive information, such as about mergers and acquisitions
- Intellectual property, or
- Financial information.

Now, especially with the advent of the GDPR, there is increasing emphasis on protecting the personal data held by organisations – whether it is about customers, citizens, staff or other individuals. To adequately mitigate the risk of a data breach or non-compliance with privacy requirements, data protection needs to be factored in to decision-making at every level.

But an organisation cannot determine how best to protect its data, until it first knows what type of data it has. Unstructured data – the information generated by staff in Word documents,
spreadsheets, emails and the like – is the most difficult to protect, unless you have a systematic way of applying the appropriate information security controls.

This is where data classification comes in. Data classification is a method of categorising information, records or systems, according to the level of harm that an unauthorised disclosure could have on the organisation. Each level of classification will have
an appropriate set of information security controls, escalating in rigour commensurate with the escalating level of harm.

And conversely, organisations need to know when certain protections shouldn't apply. For example, de-identified data can be released as 'open data' by government, or sold to other organisations, or used for a new purpose such as data analytics, because privacy laws cease to apply once data has been de-identified to the point where there is no longer a reasonable chance of identifying an individual.

Information security and privacy protection objectives are now aligned: to ensure the availability, integrity and confidentiality of identified information assets, and to mitigate threats of unauthorised access and disclosure.

For unstructured data, the best way to apply the correct information security controls is for the author of the data to classify the data, at the time they generate it. When information assets are classified by their owners, controlling access to them becomes much simpler. The way documents are handled, published, moved and stored by IT systems and staff will depend on their classification – as indicated by protective markings.

"You should be fully aware of all the personal information you handle, where it is kept and the risks associated with that information before deciding what steps to take."
Office of the Australian Information Commissioner, Guide to Securing Personal Information

Protective Marking

Protective Marking refers to the marking on a piece of information or communication (such as an email) that identifies its degree of confidentiality - think of folios in spy thrillers marked TOP SECRET. These markings, also known as security classification labels, convey the level of sensitivity of documents or communications to the people and IT systems handling them.
The international standard for information security management, ISO 27001, defines procedures for labelling and applying classifications when handling files and communications. Protective marking is an effective way to ensure that systems and staff are aware of security requirements for specific files. In commercial and government environments, information assets are typically marked with one of four classifications:

Level 0 - Public (or unclassified)
Level 1 - In Confidence
Level 2 - Confidential
Level 3 - Highly Confidential (company secret)

More or fewer levels of classification may be used depending on an organisation's needs, and the name of each classification can also vary between jurisdictions.
Some jurisdictions also use a set of Dissemination Limiting Markers (DLM) on information that poses a low enough level of harm to remain 'unclassified', in order to indicate that the information should nonetheless not be made public without review. DLM protective markings might include 'For Official Use Only', or 'Sensitive: Personal'.

"Protective markings act as an important visual signal…. indicating the minimum security controls to be applied during the use, handling, storage, transfer and disposal of information."

Victorian Commissioner for Privacy and Data Protection,
Guidelines to protecting the security of personal information

Protecting Data, Even While Sharing Data

Data sharing is crucial to the way modern organisations work, with cloud computing, mobile devices and social media each adding multiple avenues for sharing information. Yet email is still the major conduit for business communications, and tends to carry information either in the text or in attachments. Data classification is a very simple means of restricting access to sensitive information in emails and attached documents, to help ensure compliance with privacy and data protection regulations.

One benefit of protective marking is that staff are frequently reminded that they're handling information that is critical for the organisation, and this raises the security awareness across the whole organisation. Another is that IT systems such as email gateways and databases have simple and clear criteria for controlling information access and distribution.

For example, emails with security classification markings can be examined by email gateways and blocked, quarantined, encrypted or allowed to pass, as determined by your security policy.
The legal, reputational and operational benefits of protective marking include:

- Prevention of accidental or deliberate leakage of sensitive information
- Protection of valuable Intellectual Property and corporate information assets
- Raised security awareness in staff, which drives an improved security culture
- A low cost solution that's simple to deploy, configure and manage.

Many government agencies and commercial enterprises, from Japan and Australia to the United Kingdom, have adopted simple classification systems that add protective markings to emails and documents, according to their sensitivity.

1. Article 83, Council of the European Union, General Data Protection Regulation, 2016/679.
2. Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, May 2014,
3. Boston Consulting Group, Unleashing the value of consumer data, BCG Perspectives, January 2013.
4. Article 33, GDPR.
5. Article 34(3)(a), GDPR.
6. U.S. Department of Health and Human Services, Press Release: Lack of timely action risks security and costs money, 1 February 2017.

Practical Example - Australia Protective Markings Enabling Privacy Compliance

Australian Privacy Principle (APP) 11 deals with the security of 'personal information'. APP 11.1 requires both businesses and federal government agencies to "take such steps as are reasonable in the circumstances" to protect personal information from loss, misuse and unauthorised disclosure.
To comply with APP 11.1, the Australian Privacy Commissioner expects "active measures" to secure data and records from loss, misuse or unauthorised access, with additional measures expected in relation to a special class of data recognised in Australian privacy law as 'sensitive personal information', which includes information about a person's health, disability, ethnicity, religion, sexuality or criminal record.

The Privacy Commissioner's guidelines require entities to use a combination of governance, procedures, technologies and systems to ensure that an employee does not access information they are not supposed to, and does not carry out an unauthorised disclosure of personal information. Emails in particular are called out as raising the risk of unauthorised disclosure, and the Privacy Commissioner therefore expects procedures to be developed to manage the transmission of personal information by email.

The privacy law then dovetails with the prevailing information security standards. The Privacy Commissioner has made it clear that compliance with the Australian Government's protective security requirements under the Australian Government Security Classification System, and the Australian Signals Directorate's Australian Government Information Security Manual (ISM), are an important aspect of ensuring compliance with APP 11. The Privacy Commissioner also expects compliance with ISO 27001, and other information security standards as relevant to the organisation.

Taking the example of the Australian Government Security Classification System, there are five levels of data classification from UNCLASSIFIED to TOP SECRET, as well as five types of Dissemination Limiting Markers, (or qualifiers, depending on your terminology) to be used as applicable on both classified and unclassified information:

- For Official Use Only
- Sensitive
- Sensitive: Cabinet
- Sensitive: Legal, and
- Sensitive: Personal

Compliance with Protective Marking Controls of the ISM

The DLM 'Sensitive: Personal' relates to 'sensitive information' as defined in the Privacy Act. The DLM 'Sensitive' is applicable to other information to which secrecy provisions apply, or the disclosure of which may be limited or prohibited under legislation.

Therefore, for Australian Government agencies, and Australian businesses following information security best practice, application of the protective marking DLM Sensitive, DLM Sensitive: Personal, or a security classification, is appropriate for data that contains 'personal information', the disclosure of which may be limited or prohibited under the Privacy Act 1988.

The ISM sets standards which are mandatory for federal government agencies in Australia, and considered 'best practice' for private sector organisations and other levels of government. It prescribes a large number of specific information security controls. The application of each one depends on the security classification (or DLM, in the case of unclassified information) of the information in question. Therefore, the ISM cannot be complied with until an organisation first classifies its data holdings – including for unstructured data.

It is no surprise then that the ISM itself requires the use of protective markings (whether a security classification label and/or a DLM), on both paper records and electronic-based information, as a way of preventing data breaches.

For Australian Government agencies, and Australian businesses following information security best practice, the use of protective markings is therefore a critical way of ensuring compliance with APP 11, by protecting personal information from unauthorised access, use or disclosure. Once a document or communication has had the relevant protective marking applied to it, both end users and IT systems designed to prevent data loss will be able to quickly recognise and apply the commensurate information security controls.

Further, marking a document or communication with the appropriate DLM can quickly indicate to both users and IT systems whether or not the higher legal restrictions with respect to the collection, use and disclosure of 'sensitive personal information' will apply, under APP 3 and APP 6.
In this way, data classification and the application of protective markings underpins compliance with both privacy laws and information security standards.