EPIC RDM READING LIST

by Elizabeth de Stadler

1. POPIA IS HERE

1 July 2020 is the date! Here is a blog about that:

Here is a super-useful page on the Information Regulator's website: It has every guideline, judgment, strategy and plan on it. This page has got all their media statements.

How does POPIA compare to the GDPR? You can read a white-paper on that here.

2. SO MANY DATA PROTECTION LAWS!

There are 100s of data protection laws now. DLA Piper created a handbook of *Data Protection Laws of the World*.

The IAPP is a good resource for this too.

3. BEFORE WE START, A BIT OF RISK MANAGEMENT

Watch The Meg. Check out the Institute of Risk Management South Africa – they are great on LinkedIn. Here is their 2020 Risk Report (pre-COVID-19) and here is their COVID-19 page.

We discussed a risk framework based on ISO 31000. ISO 27001 is a standard for information security management.

Here is an article about both. Some people are not fans of these standards, so here is a critical analysis of the standard.

Go play around on the McKinsey on Risk page. Their work on COVID-19 has also been great!

When I find myself saying 'not again!' it means that I am in risk management groundhog day. I wish I came up with that myself, but alas. Here is an awesome guide to the questions you should ask to break the cycle and get to the root of the problem. It was drafted for information security risks but works well with other types of risks too.

What does risk management have to do with POPIA and research data management? Everything!

The best book I have read in the last decade is *Factfulness: Then Reasons We're Wrong About the World – and Why Things Are Better Than You Think* by Hans Rosling. If you want to understand 2020, read Nicholas Taleb's *The Black Swan: The Impact of the Highly Improbable*.

4. YOU NEED TO KNOW ABOUT COMPLIANCE MANAGEMENT

Compliance risk is one of the categories of risk – this is what compliance officers and sometimes in-house lawyers, must manage. One of the implications of POPIA is that information risk is now also part of compliance risk.

The gold standard for compliance management is the Generally Accepted Compliance Practice framework.

5. WHY ARE POPIA AND RESEARCH DATA MANAGEMENT COMPLIANCE IMPORTANT?

We spoke about the cost of poor information management. Here is the article about 'the rule of 10'.

The International Association of Privacy Professionals is the best source of information for data protection. Here is an article about the Return on investment of mature privacy programmes. It refers to a study by CISCO called *From Privacy to Profit: Achieving Positive Returns on Privacy Investments*.

That is the carrot, the stick is all the data breaches. Here is a beautiful infographic. Here is the IBM *Cost of a Data Breach Report* for 2019. USD3.9 million, yikes! Here is an excellent analysis of the Target data breach which is an excellent example.

Boards are often swayed by what other organisations are worried about. The World Economic Forum does the *Global Risk Report*. Here is the 2020 edition.

6. HEALTH DATA – ALL AND EVERYTHING!

The health science sector has been dealing with the privacy aspects of research data management a lot longer than other areas – and therefore we can learn quite a lot from them!

Canada's has a lot of great resources in this area. For example, four Canadian provinces have specific legislation that governs personal health data privacy on top of legislation which governs general personal data privacy. You will find links to all four pieces of legislation here.

South Africa's National Health Research Ethics Council has also done a nice job of providing guidance on data privacy concerning health research. You can find the NHREC Ethics Guidelines here. This is a nice article which gives an overview of how the NHREC Ethics Guidelines and POPIA fit together.

7. ETHICS AND RESEARCH DATA MANAGEMENT

As I explained, privacy fits nicely into the usual ethics approval review that all research study proposals have to go through. The FAIR principles give a good overview of this. This is an article I co-wrote for the South African Medical Journal about how privacy and ethics intertwine in the health research space and 'the C-word' (Consent!!). This is another article written on the use of 'broad consent' in genomic research.

8. PRIVACY BY DESIGN

Incorporating the principles of 'Privacy by Design' into how a research project is designed is a way to incorporate privacy considerations into research data management right from the start. Here are the 7 principles of 'Privacy by Design'.

9. PERSONAL INFORMATION ASSESSMENTS

POPIA requires 'personal information assessments' in the POPIA Regulations. Overseas they are called privacy impact assessments or data protection impact assessments. The CIO has a good guideline, but we really love the *Privacy Impact Assessment toolkit* created by UCISA. Just remember, POPIA always require personal information assessments. The GDPR only requires them in certain instances.

10. CONTRACT MANAGEMENT

As we discussed, good contract management is essential to good research data management. Here is an interesting benchmarking study done on research contract management at UK universities that demonstrates this principle well.

11. SO HOW ARE OTHER UNIVERSITIES DOING RESEARCH DATA MANAGEMENT?

One of the perks of POPIA being enacted a few years after the GDPR is that we can learn a thing or two from our European and UK counterparts on how they are dealing with research data management under the GDPR. One of my new LinkedIn friends (who is a data privacy officer at the Erasmus University Rotterdam in the Netherlands) has developed these great resources about data privacy in the research space at universities which I used in my slides. You can find them in full here.

These are some additional useful resources for research data management we found at other UK universities:

- The University of Glasgow's integrated Personal Impact/ Ethics Impact Assessment guide can be found here;
- Bristol University's Research Data management Policy and Guides are really good. You can find them here and here
- Bristol University's research project screening questionnaire also provides a very nice insight into what types of situations trigger a privacy impact assessment in an academic research environment. You can find this here.
- Edinburgh University's 'Do's and Don'ts' Checklist is also helpful. You can find that here. Edinburgh University also has a really good guide on how to write a research data management plan, which you can find here.

12. AND FINALLY...WHAT ARE SOUTH AFRICAN UNIVERSITIES DOING ABOUT POPIA?

I have attached the POPIA Code of Conduct for South African public universities which has been adopted by Universities South Africa (USAf). USAf is a membership organisation representing all 26 of South Africa's public universities.

13. OTHER SOURCES

Here are the sources we use when we don't have the answer:

- IAPP
- ICO
- European Data Protection Board
- European Data Protection Supervisor
- Privacy International
- Our own website and LinkedIn profile!

Disclaimer: Just be careful! If POPIA's wording is different you need to take that into account. The international sources may be less persuasive.