White paper on GDPR

UNIVERSAL PRECAUTIONS
WHY AFRICA NEEDS TO DANCE TO THE GDPR TUNE

From 25 May 2018, consumers' rights regarding the protection of their personal data changed radically, and a new set of rules altered the way businesses, marketers and individuals deal with data. The reboot button was pushed, giving power to the people to choose which brands and teams they want to be a part of, and revoking the ability of business to collect, store and disseminate data as they choose. Here's why South Africans should apply universal precautions to their data collection...

OVERVIEW

The General Data Protection Regulation (GDPR) is designed to give individuals more control of their personal data and ensure companies that have it do all they can to prevent its mismanagement or loss.

It also sets out a path and timeline for companies to respond promptly and effectively in the event of a hack or data breach, and falling foul of these requirements could be extremely costly, both financially and reputation-wise. So, how does the GDPR stack up against our own Protection of Personal Information Act 4 of 2013 (POPIA/PoPI)? Quite simply, it enhances PoPI and raises the bar – and the consequences of non-compliance dramatically.

Just as PoPI is not limited to organisations based in South Africa – meaning that if you have information on anyone who's a South African citizen in any of your databases, PoPI applies to you – the GDPR does the same with data from EU companies and citizens.

Consumers have been sharing more personal and sensitive information about themselves on a variety of social and other online platforms, and the sheer amount of data that has been accessible to business and marketers until now is staggering. The more data there is, the more risk is involved. As technology trends like cloud, mobile, social and collaboration increase demand for data management and security capabilities, governments are stepping up with a shield of protection, and a sword of financial and reputational consequence for defaulters.

Data is no longer the "free for all able to collect" trove of information it has been until now. While many in South Africa have noted that PoPI is all hat and no cowboy, the GDPR has already flexed its muscles with a South African insurer whose data was breached, but who didn't comply with the 72 hours the GDPR has determined to be the time during which the breach must be reported. The insurer, owned by one of the Big Four banks, not only had EU shareholders, it found out about the breach when the hackers themselves alerted it with a ransom note.
The GDPR states that the onus is on every organisation that collects, stores and/or disseminates data to keep customers' personal data secure and to test security measures regularly; it notes that security must be part of the design process and not an afterthought, and that "appropriate technical and organisational measures" are required, and proactive monitoring for data breaches, along with reporting, is vital in mitigating the wrath of the European Union.

Importantly for South African organisations, GDPR regulations apply to anyone offering goods or services to anyone in the EU, regardless of your location. This applies to your website and any apps you may have, as an IP address is considered personal information. While the GDPR may be a little less stringent on smaller companies of under 250 employees, compliance is still required.
https://medium.com/@ageitgey/understand-the-gdpr-in-10-minutes-407f4b54111f

KNOW YOUR COMPLIANCE DIRECTIVES

To comply with the GDPR, the system of "Universal Precautions" – as used by the medical industry to assume the worst when dealing with undiagnosed or potentially infectious diseases – should be similarly mapped out by a Governance Committee or Data Manager. This should include the ability to flag potential hotspots where data leaks or breaches may occur, whether from outside or within the organisation.

A chain of communication is vital to meet the strict reporting deadlines set by the GDPR and also to mitigate the negative impact on the organisation's reputation once the media is informed about the breach. Even while the technical department is working on the issues at hand, top management must be dealing with GDPR and PoPI communications, as well as their own staff and the public.

All staff members who come into contact with data in any way must also understand what is required when dealing with data that is regulated by the GDPR, this being:

- Information that enables the direct or indirect identification of an individual
- Individuals' posts to any social media and other online platforms
- Data that may appear to be anonymous, but can be used to identify a person

Businesses operating in South Africa should ensure that all staff members understand that the GDPR applies to data transferred to or from the EU; essentially, it applies to businesses that are not established in the EU but offer services to EU-based citizens (either free or paid) and to websites or any other related online services accessed by EU-based individuals.

Importantly, the GDPR also applies to any organisation that holds or processes data on EU citizens, regardless of where the organisation has its headquarters, including South Africa. South African businesses who engage in business with persons in EU member states, especially those that import or export goods or services from or to European counterparts, must be compliant.

[Ref: http://www.businessessentials.co.za/2018/05/08/important-questions-answered-about-popi-act-and-gdpr/]

This being said, the chances of a South African somehow, sometime doing business with someone in the EU are great in our global village with its online markets. Keeping the GDPR requirements in mind – even just to err on the side of caution – is key. Knowing the six basic requirements will constitute part of your Universal Precautions to reduce the impact of a breach. These are:

Requirement 1: Good reason
You must have a good reason for collecting personal data, and it needs to be a reason acceptable to GDPR. Valid grounds include:

- Getting explicit consent from the user to collect the data and being able to produce such when asked for;
- The data is required to fulfil contractual obligations with the user; such as name, address and/or contact details;
- Information is required to protect someone's life;
- The data you ask for enables you to comply with another law; and/or
- You are a public authority/government department and the data enables you to carry out your duties.

Essentially, you must have an actual business need for the data you are collecting and must use the most limited justification possible and inform the user or your precise justification at the time you collect the data. Note that legal justifications have sub-sets of specific rules which must be followed, and pre-checked checkboxes and disclaimers that are not highlighted separately, as opposed to within your privacy policies, are not acceptable.

Intensely sensitive data

If you work with data considered to be extremely sensitive and do not have a GDPR expert within your company, you'd be well advised to consult a professional. This category includes:

- Health information and biometrics
- Political or trade union affiliations
- Race
- Religion
- Sexual Orientation

Requirement 2: User control

Unlike pre-25 May when businesses and marketers could collect data merely by asking a consumer for their details or by buying databases from other organisations, users must be given control over any of their data you collect, store and/or disseminate. The GDPR highlights eight specific rights of the user:

1. You must explain, in a manner understandable to the user, why you are collecting their data; what you intend to use it for; and how long you will keep it
2. Should a user requests it, you must provide them with a copy of the all data you have collected about them
3. If a user can show that their data is inaccurate, you must update it
4. You are required to delete all of a user's data, and stop processing it, should they request it
5. Users have a special right to object to their data being used for certain purposes, such as marketing initiatives
6. Any user wishing to engage with another service must be given their data on request from you, in a machine-readable format

7. Using personal data for automated decision-making or profiling exposes you to a number of different requirements regarding how your model works, having an appeal system and more – once again, engaging a professional for this will likely be the best protection for you
8. In most cases, you are required to process any of these user requests within one month

Not all of these user rights always apply and will largely depend on the reason you collected their data initially and which rights apply to which legal justifications may require explanation by a legal entity or consultant. However, if your system complies in the best way it can with these rights – those Universal Precautions - you are likely to be covered.

Requirement 3: Security of customer data

As stated earlier in this white paper, the onus is on the organisation that has collected the user information to keep this personal data secure; to test security measures regularly; and to implement the strongest possible security measures as a business imperative and not a bolt-on to digital initiatives.

Requirement 4: Data Governance and Documentation
Being able to produce documentation on all of the above is vital to maintaining proper governance and accountability should this be required in the event of a breach or cyber attack. Specifically, you need:

- Written records of your purposes for collecting data; data retention policies; history of any time data is shared; and your security policies; and
- A written contract outlining their privacy responsibilities is required from any external third party you hire to process your data on your behalf;

The GDPR requires that you conduct regular data protection audits (DPAs) to and name a Data Protection Officer (DPO). This could also form part of your Data Governance blueprint, in order for it to be produced as evidence of compliance when reporting an incident.

While GDPR sounds scary and looks cumbersome, using common sense in the process will help you to work within these parameters. The damage to reputation as well as the stiff fines doled out by the GDPR can be devastating to organisations of any size.

SUMMARY

Know your duties, risks and responsibilities to the individuals whose data you collect, as well as the rules that govern your manner of collection; use of data; and ability to respond to both users and the GDPR when requested to do so. Maintain a constant, close watch on your data by employing file integrity monitoring software which gives you better control over your data; alerts you to who is accessing it; notifies you when changes are made; and makes it easier to stay GDPR compliant. Set up data Universal Precautions as a business imperative and ensure all staff are familiar with the value of data and the importance of its owners' privacy.

Ends
Word count: 1 832