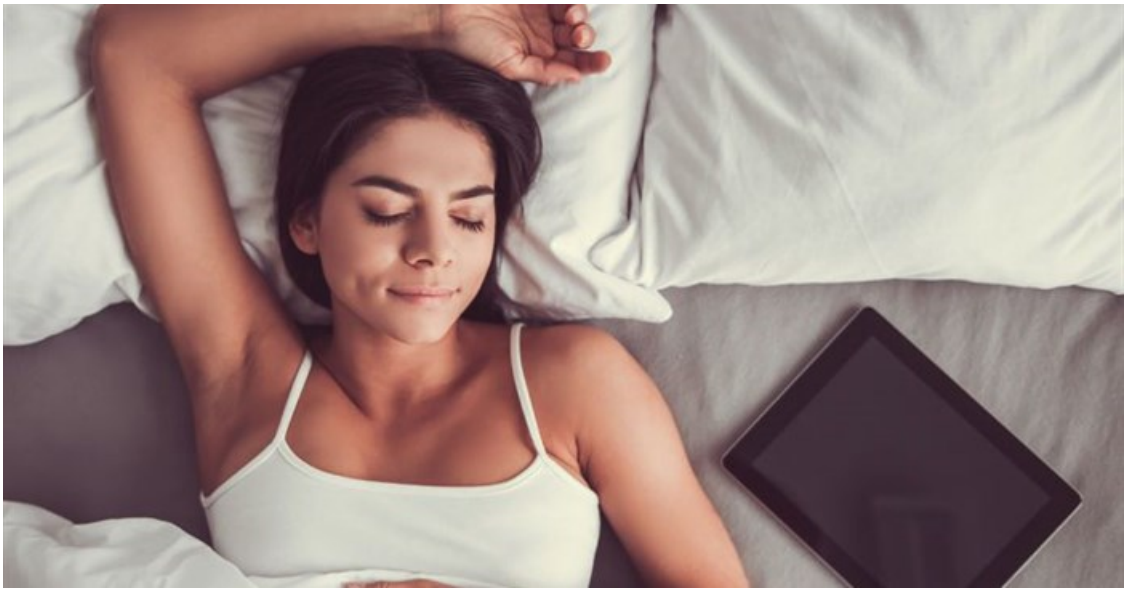
Data protection in South Africa - Sleep a little easier

By Nick Bester

18 Jun 2018

Many facets of the digital ecosystem are complex and fragmented but, as the opaque and largely unverified world of data collection comes under scrutiny and the new General Data Protection Regulations (GDPR) come into force in Europe, ignoring a data's source is no longer an option.



© georgerudy via 123RF.com

This is a new era of transparency, verification and consent, and we in South Africa are subject to the same set of rules if we offer goods and services to the European Union or monitor EU citizens.

It is vital we acknowledge we're living in an age where data is a valuable commodity. He believes protecting this information is the responsibility of any individual who handles it and is preparing for the responsible use of consumer information. Here he shares the steps he has taken to ensure the agency is top of the game in order to best protect its clients and their customers.

Starting point

Anyone who is under the impression or aware that they service EU citizens, should garner a solid understanding of what GDPR is by reviewing the official website.

Essentially, this states that the GDPR not only applies to organisations located within the EU but to those located outside of the EU, if they offer goods or services to, or track the activity of EU citizens.

What does Facebook's data breach mean for personal information and businesses in SA?

Ahmore Burger-Smidt 14 Jun 2018

It further applies to all companies processing and holding the personal data of EU citizens living in the European Union, regardless of the company's location which implies that it does apply to South African companies.

Knowing what data you're dealing with

The next step is to know what personal data you are responsible for. Personal user data is basically any information that could be used to identify, locate and contact an individual including, name and surname, email address, phone number, mobile number, GPS coordinates, physical address, postal address etc. This information is extremely sensitive and, in our day and age, it is considered a commodity which can easily be exploited by others for malicious reasons.

Interrogate your digital platforms and your company processes

You then need to determine if any platform you have developed and managed captures sensitive data for citizens of the European Union, make an extensive list of these platforms and also the technical requirements to facilitate the update for compliance.

With this in hand, define what data you are holding on behalf of these users and what you are using this information for. Generally, a business analyst or backend developer would have a good understanding of this information and will start by interrogating the databases and data structures of your platforms. Add the lists of user data under each of the platforms you control where you potentially see a breach of GDPR compliance.

Is your network ready for GDPR and PoPI?

Bryan Hamman 7 Jun 2018

Then, check if any of the user data you capture is shared or accessed by any third-party service provider. These types of services providers vary but a very common type of service provider in this context would be a bulk email campaign delivery service. Any data moving out of your systems and into the hands of another service is a major risk in data security. Document these services and why you are using them.

Now, you must turn to examine human interaction with this data. Check what data management capabilities the users on your platform have and ask yourself if these users can update and delete their data from all your systems including the third-party services used by your platforms at any time. If you can't answer this question then make a note of any platform that is affected.

When it comes to your company processes, the kinds of questions you'll need to ask include:

- Are you getting emails from clients containing Excel spreadsheets of user information? This could be a major concern if this email gets sent from person to person and somehow leaves the confines of the office.
- Do you store any user data locally on in-house server solutions which allow insecure/open access? The concerns here are similar to that immediately above but you also need to understand how the access to this information is managed and if you are establishing protocols to ensure that this information is used responsibly.

Bringing it all together

There are three major remediation steps to take.

One, when it comes to your platforms and the management of the data you may capture on these, make sure you resolve any requirements on your platforms related to functionality that impedes a user from managing his/her data captured within your platforms. This will require development and design efforts facilitated by your operational teams based on the interrogation of your platforms indicated above.

Two, establish processes and systems for data governance within your organisation. Communicate updates and facilitate training to ensure the new regulations and requirements are understood and applied.

Three, address the legal documentation. For example, update your platform privacy policies and terms and conditions. Ensure that all your platforms and third-party service providers which are used on these platforms are indicated in the documentation to ensure that the exact nature of the usage of user data is defined. Communicate to your user base that you have updated these legal documents on these platforms and that they comply with the new GDPR regulations.

Closing the loop

The final step is to ensure that all marketing related functionality on your platforms defines the specific engagement a user will have with your platform by using ‘opt-in’ methods such as the acceptance of terms and conditions and privacy policies by tapping a checkbox. These ‘opt-in’ legal documentation should detail why you’re capturing the user data, how you’re going to use this data and lastly, which additional services this data will be exposed too.

Do your research on GDPR, there are many resources online which can help and be aware GDPR has already come into effect as of 25 May 2018. Even if you aren’t affected by GDPR, you should be looking at the user data you capture very carefully to ensure you protect this information and to ensure you comply with PoPI, if you haven’t already done so.

ABOUT NICK BESTER

Nick Bester has 14 years of experience in design, development and implementation of digital marketing solutions ranging from virtual reality, 3D projection mapping, mobile apps, social media strategy, web platforms and digital activations for clients including Nike, MTN, SAB Miller, KFC, Vodacom, Cell C, South African Tourism, Toyota, Lexus, PPC, Nelson Mandela Foundation and DStv.

- Data protection in South Africa - Sleep a little easier - 18 Jun 2018

View my profile and articles...

For more, visit: https://www.bizcommunity.com