Data Protection and Privacy: GDPR vs POPIA

Introduction

Who owns your data? From corporations to criminals, there is no shortage of people trying to access the information you generate online. While many feel unable to protect their information from companies like Google and Facebook, for instance, it does not have to be a losing battle. Understanding data privacy and security is the first step to maintaining your digital autonomy (Higgins, 2020).

Data privacy is how we choose to maintain our privacy online- in a world where information is a highly sought-after commodity (and it is 'virtually' everywhere). It is therefore vital to know who is viewing our activities online as well as what they're doing with that information. Allowing larger companies to track and store your data can have unexpected consequences, so you should have a say in the matter (Higgins, 2020).

While it may be easy to focus on the dangers of hackers and malicious actors… that's only the half of it. Protecting your privacy is just as important as maintaining your data security.

It's worth defining the difference between "data security" and "data privacy". Though similar, these concepts are different (Higgins, 2020):

- Data Security is the protection of data from criminal activity and deliberate hacks.
- Data Privacy covers how data is legally gathered, stored, and used.

It's easy to focus on security, since the dangers involved seem more pressing. Cyberattacks are on an unprecedented rise. From phishing to password cracking to IP spoofing, there are many strategies that hackers can use to steal your data. However, when it comes to corporations and legitimate online services, people feel less certain about how to maintain their autonomy and privacy. Companies are (usually) not breaking the law, and you are probably using a product that you signed the terms and conditions for.

The extent to which your data is legally protected varies depending on where you are (in the world). Whether in the UK, US, or even In South Africa- there are different data protection laws in place. In this paper, we will be look specifically at the POPI and GDPR acts which have been implemented in South Africa and the EU, respectively.
We will also explore the guidelines for online research set out by ESOMAR- the global voice for data, research, and insights community. Furthermore, it is a membership organisation speaking on behalf of over 4900 individual professionals and 500 companies who provide or commission data analytics and research in more than 130 countries, all of whom agree to uphold the ICC/ESOMAR International Code. Thus, promoting high standards of ethical behaviour and further reinforcing public confidence in research.

What is POPIA?

The Protection of Personal information Act (POPIA) is the comprehensive data protection legislation which was signed into law in South Africa in November of 2013 (alt, 2017).

Who are the Role Players?

The Protection of Personal Information Act (POPIA) involves three parties (who can be natural or juristic persons (a non-human legal entity/ organisation that is authorised by law with duties and rights- having a distinct identity)) (Michalsons, 2017):

- **The data subject**: the person to whom the information relates.
- **The responsible party:** the person who determines why and how to process information. For example, profit companies, non-profit companies, governments, state agencies and people. Called controllers in other jurisdictions
- **The operator:** a person who processes personal information on behalf of the responsible party. For example, an IT vendor. Called processors in other jurisdictions.

The Protection of Personal Information Act places various obligations on the responsible party, which is the body ultimately responsible for the lawful processing of personal information. Responsible parties should only use operators that can meet the requirements of lawful personal information processing prescribed by the Protection of Personal Information Act (Michalsons, 2017).

Consumers who may find themselves concerned about their personal information can breathe a sigh of relief as President Cyril Ramaphosa has proclaimed sections of the Protection of Personal Information Act into law as of June of 2020 (Mahlati, 2020).

While much of the Act's components were put into effect in April 2014, other sections had to be halted until other measures were put in place. As part of the Act's requirements, an Information Regulator was established, and its members took office in December 2016. Therefore, now that an Information Regulator has been established it has paved the way for other sections of the Act to come into effect. These sections include Sections 2 to 38; sections 55 to 109; section 111; and section

114 (1), (2) and (3) will commence on 1 July, 2020. Sections 110 and 114(4) will commence on 30 June, 2021(Mahlati, 2020).

The various sections deal with the following components:

The sections which will commence on 1 July, 2020 are essential parts of the Act and comprise segments which pertain to, amongst others, the conditions for the lawful processing of personal information; the regulation of the processing of special personal information; Codes of Conduct issued by the Information Regulator; procedures for dealing with complaints; provisions regulating direct marketing by means of unsolicited electronic communication, and general enforcement of the act (Mahlati, 2020).

Furthermore, Section 114(1) is of particular importance as it states that all forms of processing of personal information must, within one year after the commencement of the section, be made to conform to the Act. This means that entities (both in the form of private and public bodies) will have to ensure compliance with the Act by 1 July, 2021 (Mahlati, 2020).

The Presidency stated that public and private bodies that process personal information will have to ensure that they do so in a lawful manner to safeguard against the theft of personal information and data breaches.

The powers afforded to the Information Regulator of South Africa may see non-compliant entities face censure should they fail to follow measures to protect private information. (Mahlati, 2020).

Who is Affected?

Any natural or juristic person who processes personal information, including large corporate and government. The data protection laws of many other countries exempt SMEs, but not currently in South Africa. Perhaps, in time to come, the Information Regulator will exempt some natural person and SMEs from complying (Michalsons, 2017).

Steps Required in Order to Comply

Responsible parties will have to take various steps to comply. For example (Michalsons, 2017):

1. Appoint an Information Officer.
2. Draft a Privacy Policy.
3. Raise awareness amongst all employees.
4. Amend contracts with operators.
5. Report data breaches to the regulator and data subjects.
6. Check that they can lawfully transfer personal information to other countries.
7. Only share personal information when they are lawfully able to.

What are the Penalties for Non-Compliance?

There are essentially two legal penalties or consequences for the responsible party (Michalsons, 2017):

1. A fine or imprisonment of between R1 million and R10 million or one to ten years in jail.
2. Paying compensation to data subjects for the damage they have suffered.

It is less likely that anyone will go to jail, and the fines are small compared to other jurisdictions. The other penalties include:

- Reputation damage
- Losing customers (and employees)
- Failure to attract new customers

Under POPIA, researchers will only be allowed to send unsolicited electronic communications to persons who have provided their consent or who are existing customers. A market researcher will only be allowed to send unsolicited communications to someone on the basis that they are a customer if the organisation has obtained the customer's contact details in the context of the sale of products or services and it relates to similar products and services that the researcher is considering for their particular project.

Furthermore, the customer must be provided with the opportunity to opt-out, which must be free and informal, at the time of collection of the information and on the occasion of each communication (Adams & Adams, n.d.).

What is GDPR?

The European Union has enacted legislation across all its member states, although individual countries have developed their own standards on top of this. The General Data Protection Regulation law (GDPR) is at the heart of the EU's privacy controls (Nadeau, 2020).

GDPR is a regulation that requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. And non-compliance could cost companies dearly (Nadeau, 2020).

The Lawful Bases for Processing Information (Boughton, 2019):
Researchers and data processors need to understand the lawful basis on which they are processing information and be clear on which they are using and why. This can be broken down as follows:

- **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose

- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations)
- **Vital interests:** the processing is necessary to protect someone's life
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law
- **Legitimate interests:** the processing of the data is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (If you are choosing to process data on this basis, you must undertake a legitimate interests assessment to show that you've considered the interests of the data subjects and are confident that you exercising your legitimate interests isn't to the detriment of their interests.)

When it comes to market research, it is vital that you ensure that you document it all so you can be confident you have selected the right lawful basis and can justify it in writing. This means that you will need to have reasoned, documented, and thought-through reasons as to what you are doing and why.

Transparency and Individual Rights (Boughton, 2019):

When it comes to market research and GDPR, agencies should also strive to be transparent about exactly what information will be stored, how long it will be stored for, for what purposes it will be used and who will see it/use it. Make sure you have a clear process for handling your response when data subjects contact you to exercise one or more of their rights – it is crucial that your staff understand the policy and are trained on their roles.

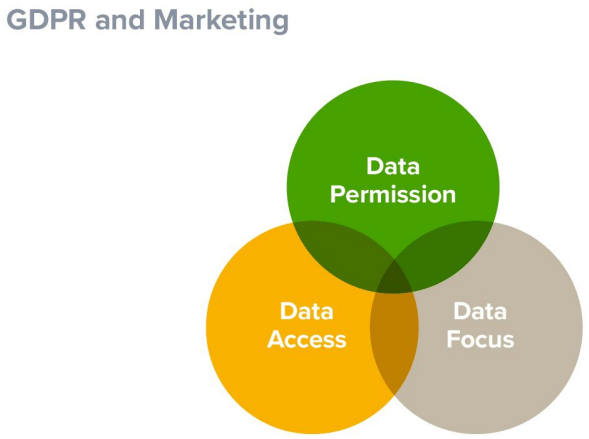
Generally speaking, market research agencies will process data for the following reasons: inviting people to participate in market research, contacting them to help find other respondents, providing technical or incentive support, supplying incentives and allowing a moderator or interview to contact respondents. And they should also provide the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

One way to ensure you are completely transparent and providing the necessary rights is to allow granular consent as much as you can to make sure all respondents know exactly how their personal information will be used. Make sure you're upfront about everything, from a breakdown of the type of information stored, to how long it will be stored for, as well as details of any third parties, and a clear indication of how they will process data.

GDPR- Key Areas

On the surface, GDPR might seem extreme, especially for smaller businesses or solo practitioners. Realistically though, there are only 3 key areas that researchers need to worry about – **data permission**, **data access** and **data focus**.



MacDonald (2017)

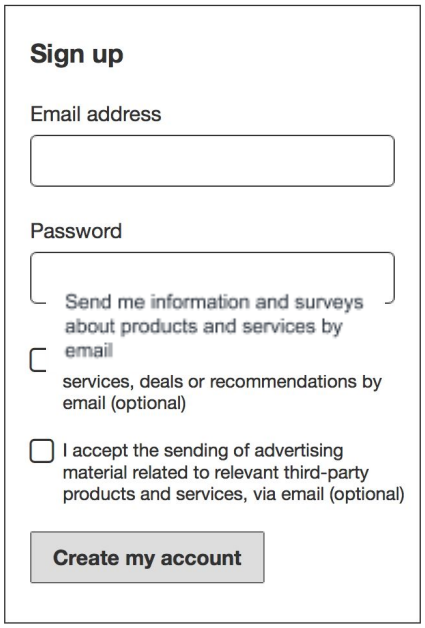
1. Data Permission

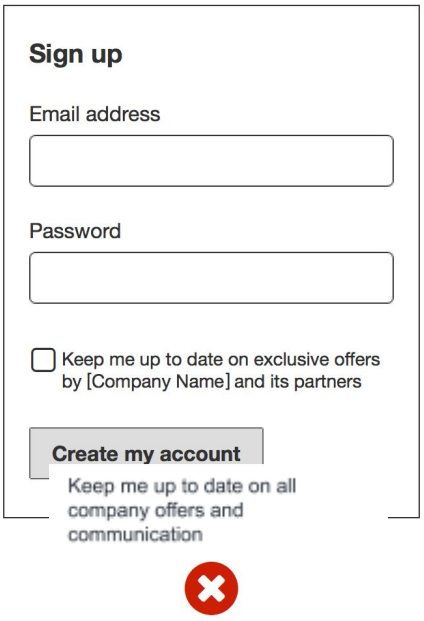
Data permission refers to how you manage email opt-ins

In practice, it means that leads, customers, and partners, need to physically confirm that they want to be contacted. You will therefore be required to make sure you have actively sought (and not assumed) permission from your prospects and customers, thus confirming that they want to be contacted.

Therefore, a pre-ticked box that automatically opts them in will not cut it anymore – opt-ins need to be a deliberate choice.

> **Below is an example of compliant vs non**-compliant opt-in options:
>
> (Instead of assuming that participants who fill out a web form want to receive surveys or marketing emails from you (right), we now ask visitors to specifically opt-in to newsletters or surveys by specifically ticking the sign-up box (left).)





2. Data Access

The right to be forgotten has become one of the most talked about rulings in EU Justice Court history. This gives consumers the right to have outdated or inaccurate personal data removed and has, in some instances, already been implemented by companies like Google, who were forced to remove pages from its search engine results in order to comply.

The introduction of GDPR offers individuals (the customer) a method to gain more control over how their data is collected and used – including the ability to access or remove it – in line with their right to be forgotten.

It is therefore, the responsibility of the market research organisation to ensure that all users can easily access their data and remove consent for its use.
Practically speaking, this can be as straightforward as including an ***unsubscribe link*** within your email marketing template and linking to their customer profile that allows users to manage their email preferences

3. Data Focus

As researchers, we may be guilty of collecting a little more data from a person than we actually need. Rather, take a moment to ask yourself, "do I really need to know someone's favourite colour before they subscribe to our annual survey?" Perhaps not.

With this in mind, GDPR requires you to legally justify the processing of the personal data you collect.

What this means is that you need to focus on the data you need and stop asking for the "nice to haves". If you really need to know a participant's shoe size and inside leg measurement, and can prove why you need it- that is, you have a specific question that needs to be answered for a particular reason- then you can continue asking for it. Otherwise, try to avoid collecting any unnecessary data and stick with the necessary information.

ESOMAR & Research Guidelines

It is essential to make the distinction between 'marketing' and 'market research'. The essential element of this distinction between market research and other activities such as advertising, sales promotion, direct marketing, direct selling, is that market research has no interest in the identity of respondents. Respondents are selected as representatives and their data is used in statistical tabulations to provide insight to a particular question/topic. The data about individual identified respondents is confidential and not passed on to the commissioning organisation (ESOMAR, 2009). Other commercial activities might appear to be similar to market research – they contact people, ask questions, and record the data. However, their major priority is to discover the personal identity of the people they contact and to use the data collected to target marketing or sales approaches (ESOMAR, 2009).

Ethical Issues in Market Research and Data Collection (ESOMAR, 2011):

Handling personal data
Data provided by respondents is confidential and the identity of respondents must be protected. The identity of respondents must not be revealed to the user of the information without respondents' explicit consent and the researcher must ensure that information is collected for specified research purposes and not used in any manner incompatible with these purposes. No personally identifiable information may be used for subsequent non-research purposes such as direct marketing, list-building, credit rating, fund-raising or other marketing activities relating to those individual respondents.

Personal identifiers
A respondent's e-mail address or other personal identifiers (e.g. screen, username, or device identifier where it is recorded in the data) are personal data and must be protected in the same way as other identifiers.

If all data which could lead to the identification of an individual are removed from data records (including identifying serial numbers which link to a separate file of identity data) the data set no longer contains personal data and is no longer subject to the requirements of data protection and privacy laws or to early deletion.

Notifications and e-mail

Researchers must remain mindful of concerns about privacy and intrusion and not make unsolicited e-mail approaches to potential respondents even in countries where this is still permitted by the law unless individuals have a reasonable expectation that they may be contacted for research.

Specific requirements
The general principle is that market researchers will not use unsolicited e-mails to recruit respondents for research purposes whether consumer or business-to-business.

Researchers are required to verify that individuals contacted by e-mail for research have a reasonable expectation that they will receive communication for research. Such agreement can be assumed when all of the following conditions exist:

- A substantive pre-existing relationship exists between the individuals contacted and the research organisation, the client or the list owners providing sample for the research (the latter being so identified)

- Individuals have a reasonable expectation, based on the pre-existing relationship, that they may be contacted for research

- Individuals are offered the choice to be removed from future electronic contact in each invitation in a clear and distinct way and this must be free of charge and easy to implement

- The invitation list excludes all individuals who have previously taken the appropriate and timely steps to request the list owner to remove them.

Researchers must not use any deception in obtaining electronic addresses of potential respondents, such as collecting e-mail addresses from public domains or under the guise of some other activity or using technologies or techniques to collect e-mail addresses without individuals' awareness.

Researchers must not use false or misleading return e-mail addresses when recruiting respondents over the internet.

Unsolicited survey invitation e-mails may be sent to business-to-business research respondents provided that researchers comply with points 3 and 4 above, as well as the anti-spam policies of their internet and e-mail service providers. This also applies to e-mail addresses of professionals whose details have been published in the public domain - e.g. lists of doctors or lawyers.

Special Issues (ESOMAR, 2015).

Collection of data from children
National rules setting the ages at which parental permission is no longer required vary substantially. Researchers must consult national laws and self-regulatory codes in the jurisdictions where the data will be collected to determine when parental permission is required or where cultural sensitivities require particular treatment. In the absence of national guidelines, consult the ESOMAR guideline, Interviewing Children and Young People.

Collecting data from children requires verifiable permission from the child's legal custodian. The parent or responsible adult must be provided with sufficient information about the nature of the research project to enable him or her to make an informed decision about the child's participation.

The researcher should record the identity of the responsible adult and his or her relationship to the child.

Business-to-business research
A substantial number of research projects involve collection of data from legal entities such as businesses, schools, non-profits, and similar organisations. Such research often involves the collection of information about the entity such as revenue, number of employees, sector, location, and so forth.

In all of these instances the participating organisations are entitled to the same level of protections from identity disclosure in reporting, as those afforded individual persons in other forms of research.

It is worth noting that many national data protection laws regard an individual's title and workplace contact information as personal data. Some data protection laws go further by applying their requirements to natural *and* legal persons.

Photographs, audio, and video recordings
A number of new research techniques create, store, and transmit photographs, audio, and video recordings as part of the research process. Two prominent examples are ethnography and mystery shopping.
Researchers must recognise that photographs, audio, and video recordings are personal data and must be handled as such. If researchers ask participants to provide information in these forms, they also should provide guidance on how to reduce collection of unsolicited data, especially from non-participants.

Finally, some types of observational research may involve photographing, videoing, or recording in public settings involving people who have not been recruited as research participants. In such instances, researchers must gain permission to share such images from those individuals whose faces are clearly visible and can be identified. If permission cannot be obtained, then the individual's image should be pixelated or otherwise anonymised. In addition, clear and legible signs should be placed to indicate that the area is under observation along with contact details for the individual(s) or organisation responsible. Cameras should be sited so that they monitor only the areas intended for observation.

Cloud storage
The decision to store personal data in the cloud should be considered carefully. Researchers must assess the cloud storage service provider's security controls and its standard terms and conditions. Many cloud storage service providers offer weak indemnities in the event that they cause security breaches and personal data are compromised. This means that the researcher's firm would be taking on considerable risk of financial damages and losses arising from serious privacy breaches that result in harm to the affected individuals.

Researchers should therefore implement compensating controls to protect against such risks. For example, they should encrypt personal data while in motion (transferred to/from the cloud) and at rest (stored on the cloud provider's servers).

Researchers should also consider purchasing a cyber-liability insurance policy.
Researchers also must consider the physical locations at which personal data are stored to determine whether use of cloud storage is a trans-border transfer. Some cloud service providers offer country-specific storage locations that may be appropriate in some instances.

Finally, researchers should locate personal data on a private cloud, rather than a public one. A private cloud is one in which dedicated equipment in a particular data centre is assigned to the researcher's firm. The main benefit of a private cloud is that the researcher always knows where the personal data are located. By contrast, a public cloud may result in data being located in two or more data centres and two or more continents, thereby raising possible compliance issues, both with applicable requirements under data protection laws and with contracts that are entered into with data controllers, which specify where personal data must be located.

Anonymisation and pseudonymisation
A key part of a researcher's data protection responsibility is to de-identify data prior to release to a client or even the general public. Anonymisation is one safeguard that involves either the deletion or modification of personal identifiers to render data into a form that does not identify individuals. Examples include blurring images to disguise faces or reporting results as aggregated statistics to ensure they will not make it possible to identify a particular individual.

Pseudonymisation involves modifying personal data in such a way that it is still possible to distinguish individuals in a dataset by using a unique identifier such as an ID number, or hashing algorithms, whilst holding their personal data separately for checking purposes. When employing such techniques, researchers should consult local national laws and self-regulatory codes to determine which elements must be removed to meet the anonymisation/pseudonymisation legal standard for such data.

Checklist- Data Protection Policy and Procedures (ESOMAR, 2015):

The intent here is to express the principles in language and in an order that is more familiar to researchers. Users also may recognise that the items are interrelated and sometimes overlapping. Nonetheless, it is essential that the checklist be viewed as whole and individual items seen as complementary rather than exclusive, paying special attention to differences that depend on whether an organisation is acting as a data controller or a data processor. Any question for which the answer is not "yes" signals a potential gap in a privacy protection programme and therefore a potential risk of violating one or more data protection laws (ESOMAR, 2015).

Minimum Impact

1. When designing a research project, do you limit the collection of personal data, to only those items that are necessary to the research purpose and ensure they are not used in any manner incompatible with these purposes?

2. Do you implement processes that ensure that research participants are not harmed or adversely affected as the direct result of cooperating in a market research project?

3. If you plan to use subcontractors or other third-party suppliers to perform services on your behalf, do you disclose the minimum amount of personal information that is necessary for them to perform the agreed upon services? Do you have contracts in place that ensure a similar level of protection on their part?

Notice and Consent

4. *Do you obtain consent from every participant whose personal data are to be collected?*

   Consent must be:
   - free (voluntary and able to be withdrawn at any time);
   - specific (relating to one or more identified purposes); and
   - informed (in full awareness of all relevant consequences of giving consent).

   Consent must also be clearly indicated by a statement or action by the research participant having been provided with the information set out under items below. Therefore, the individual should be informed about:

   - the use to which his or her personal data will be put
   - the specific data to be collected
   - the name, address, and contact information of the company or organisation collecting the data and, if not the same organisation, the data controller
   - whether data will be disclosed to third parties.

5. Are you clear about the purpose or purposes for which the data are collected and maintained?
6. Are you clear about the specific data to be collected?
7. Do you make clear how the data will be collected, including any passive data collection of which the participant may not be aware?

Integrity/Security

8. Are procedures in place to ensure that all personal data collected are accurate, complete, and up to date?

9. Do you ensure the personal data are preserved no longer than is required for the purpose for which the information was collected or further

processed? Do you have procedures to separately store or remove identifiers from data records once they are no longer needed?

10. Are there procedures in place for responding to requests from individuals about personal data you may have collected from him or her? Do your procedures for handling access requests from individuals include authenticating their identities, responding to their requests in a reasonable period of time, allowing them to correct inaccurate data or deleting the data entirely?

11. Are there security protocols in place for each data set that protect against risks such as loss, unauthorised access, destruction, use, modification, or disclosure?

The use of appropriate security safeguards to provide necessary protection includes:

- physical measures (locked filing cabinets, restricting access to offices, alarm systems, security cameras)
- technological tools (passwords, encryption, firewalls)
- organisational controls (background checks, rules relating to taking computers off-site, limiting access on a "need-to-know" basis, staff training, agreements with clients and subcontractors)

12. Is there a clear statement on how long personal data are retained?

Transfer of Data

13. Do you have defined rules and procedures governing the use and disclosure of personal data?
14. Are the conditions under which personal data may be disclosed clear and unambiguous?
15. Are your staff aware of those rules and trained in how to implement the procedures?

Trans-Border Transfers of Personal Data

16. If personal data are to be transferred from one jurisdiction to another, is it done in such a way that it meets the data protection requirements in both the origin and destination jurisdictions?

Outsourcing and Sub-Contracting

17. Are there clear requirements including appropriate oversight for any outside data processors or other subcontractors?

Privacy Policy

18. Is information about your privacy and personal data protection programme readily available and in a form that is easily understood by participants?

19. Is the identity and responsibility of the data controller clear?

20. Is it clear that the data controller is accountable for personal data under its control regardless of the location of the data?

Researchers must review and comply with the national data protection and market research self-regulatory requirements the particular country or region wherein they plan to conduct their research or process data. The guidance provided above is a minimum standard and may need to be supplemented with additional measures in the context of a specific research project.

Hyper-Personalisation vs Legislation

While legislation has been put in place to protect both businesses and the public, customers are looking for more personalisation when it comes to their service providers. But, why do customers have this expectation?

The expectation for personalised services has been set by organisations (such as Netflix or Kindle) who have effectively personalised their services for their valued clients. Personalisation has been dominating the retail conversation in recent years- and for good reason. The trend of tailoring sales and marketing campaigns towards individual shoppers and their needs/desires (Boyle, 2018).

The goal of a customer-centric marketing strategy is to make your marketing efforts feel honest and organic instead of like a thread of 'mad-libbed' emails. The challenge lies in delivering a truly personal experience to every customer (Boyle, 2018). Furthermore, extreme personalisation attempts to personalise as many details as possible of the customer experience across every channel. However, personalisation can also go too far, and runs the risk of overwhelming the customer.

Therefore, as organisations pursue 'personalisation' to ever greater degrees, it's essential they understand how it could negatively impact both operations and consumers. For instance, over-personalisation can (Boyle, 2018):

- **Distract from other business opportunities**- Personalisation is a major ongoing effort, which often leads retailers to focus on certain segments of consumers over others. That can lead to more repeat sales or an increase in a particular type of consumer but can attract fewer new customers overall.
- **Annoy target customers-** There is a fine line between a personalised message and an unwanted sales pitch—or worse yet, a breach of privacy. Retailers who are overzealous about personalisation risk alienating consumers with endless emails and push notifications that are uncomfortably relevant, and ultimately irksome.

- **Make mistakes in outreach efforts**- The detail-oriented nature of personalisation makes it ripe for error. This may include adding the wrong name, location, or

product interests making the entire outreach effort seem shallow in the minds of consumers.

- **Compromise the customer experience**- In a brick-and-mortar setting, extreme personalisation takes a huge amount of input. If you do manage to create an in-depth experience for one customer, but can't replicate it for everyone, it could cause others to feel neglected or ignored.

- **Hurt the omnichannel**- Consumers may expect to have similar experiences across sales channels. It may be easy to personalise the online experience but harder to translate that in-store, which means personalisation can compromise a broader omnichannel strategy.

- **Commit too much to customers**- Once customers are exposed to personalisation through one sales cycle or channel, they may expect it at all times. Retailers who are not able to commit to an ongoing personalisation effort could set consumers up for disappointment.

It is not just hyper-personalisation that can be taken too far, in fact, the collection and use of that information can also be taken too far, and sometimes, there is a complete misuse of customer information. So, where do we draw the line in terms of data collection and the use of that data?

We must bear in mind that existing customers may be more comfortable with a certain level of invasiveness as in comparison to potential customers. So, the way in which you use that data is critical:

- Existing Customers- Data is used to build and further maintain the relationship
- Potential Customers- Data is used to start the conversation.

So, what does legislation mean for your success in CX? Well. legislation can either be seen as an obstacle that needs to be overcome, or you can see it as a competitive advantage, helping you stay within certain parameters while still being able to collect and make use of personal information effectively and of course, legally - a tool in your arsenal, perhaps.

Conclusions

With increasing public concerns about the importance of individuals being able to control how their personal data is used and for what purpose comes a pressing need for clear ethical and professional guidance on how to handle that data responsibly.

While in theory, extreme personalisation can distinguish a brand and surge sales, in reality, this process could actually compromise the consumer experience (Boyle, 2018). We believe that legislation with trust can lead to positive outcomes. It is essential that you empower your customers by educating them about their rights to data privacy as well as show your customers that they are in control of their data and what you are doing to ensure the safety of their personal information.

One thing that has remained constant, however, is the need for researchers to protect the reputation of market, social, and opinion research through practices that ensure transparency for respondents and clients, maintain confidence in the information they provide, and demonstrate consideration for research participants.

And, while there may be hefty fines or penalties for non-compliance, your main motivation for complying with the Protection of Personal Information Act (POPIA) should be to protect people from harm. It is more important than ever before to maintain public confidence in research and to continue to demonstrate our recognition of the ethical, professional, and social responsibilities that come with using people's personal data (ESOMAR, 2016).

With regulations such as the POPIA and GDPR being enacted in the respective countries, ensuring that the sensitive data that customers share with organisations are well protected has become somewhat easier, with particular rules in place to maintain anonymity and/or privacy. Thus, ensuring the responsible handling of data.

References

Adams & Adams (n.d.). *Will privacy laws like GDPR and POPI kill the direct marketer?* Adams & Adams

Alt (2017). *POPIA Compliance*. Altadvisory Africa.

Boughton, L., (2019). *Back to Basics: Everything You Need to Know About GDPR in Market Research*. Angelfish Fieldwork

ESOMAR, (2009). *Guide on Distinguishing Market Research from Other Data Collection Activities.* World Research Codes and Guidelines.

ESOMAR, (2011). *ESOMAR Guideline for Online Research*. World Research Codes and Guidelines.

ESOMAR, (2017). *ESOMAR Data Protection Checklist*. World Research Codes and Guidelines. https://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ESOMAR-Data-Protection-Checklist_September-2017.pdf

ESOMAR, (2016*). ICC/ ESOMAR International Code- on Market, Opinion and Social Research and Data Analytics*. World Research Codes and Guidelines.

Higgins, M., (2020). *Why Data Privacy is Important*. NordVPN

MacDonald, S., (2017*). GDPR For Marketing: The Definitive Guide For 2020.* Super Office.

Mahlata, Z., (2020). *Ramaphosa Paves the Way for New Data Protection Laws with POPi Act*. Independent Online and Affiliated Companies. IOL.

Michalsons, (n.d). *Protection of Personal information Act Summary- POPIA*. Michalsons.com

Nadeau, M., (2020). *General Data Protection Regulation (GDPR): What You Need to Know to Stay Compliant.* CSO Online.