POPIA Worskhop - CPD accredited

Q&A - as answered during the presentation

Financial Intermediaries Association of Southern Africa

Question	Answer(s)
What is the position on One Drive and iCloud storage?	Micorosft OneDrive is typically stored in the EU or could even be in South Africa - and would be deemed as being stored ni a jurisdiction where the laws are equal to or better than POPIA. iCloud would most likely in be in the USA - the USA has both federal and state laws to protect US citizens. YOu need to ensure that the T&Cs and Privacy statement of both these platforms are clearly understood to confirm that they apply security and privacy meaures adequatly.
What should we do when a client requests that personal data be deleted, but some other legislation requires that we keep the data for a certain period of time?	Where another Act requires that you maintain information of your clients for an extended period after it is no longer needed such as FAIS (5yrs) or the Companies Act (7yrs) you may decline the request based on the requirements as defined in the supporting Acts.
if I have a existing book of clients and want to move over to other broker how will POPIA impact that. Can it be done by requiring a book transfer, brokers appointment or something else?	If I understand your question correctly, the clients must be notified if the reason for moving is not optional. If it optional, we must get consent
How will the requirement to destroy information after 5 years impact on the proof needed by Medical Schemes of previous medical scheme memebership with membership certificates of previous Medical schemes	POPIA permits the retention of information for as long as we require the information. Such a requirement by a regulator is a good reason to retain. We will need to ensure the information is kept securely and updated. Eventually all regulators will align as POPIA applies to them as well. Regulators are also responsible parties.
Does the act mention anything regarding hard copy documentation and the disposal of such? For example, does hard copy documents with personal information need to be shredded before being disposed of? (of course it would be best practice to do so, but does the act mention anything in this regard?)	Yes - a record in the Act is defined broadly as any medium that contains PI/SPI, and importantly irrespective of when it came into being or under your control.
Would a third party CRM/Quoting system provider (atWork, MMX, Tial, etc) be considered an Operator?	Yes, where any third party processes information on your behalf and authority they would be deemed an operator.
If FICA requlations conflict with POPIA, which act prevails? for example the designation PEP would in my view conflict with POPIA?	POPIA does not apply to some processing of information for purpose anti-money laundering and counter terrorist financing. We will need to store it securely and report to Information regulator and data subject is accessed by unauthorised persons.
How do you suggest a small brokerage dicate terms to product suppliers? This is not practically possible. Product suppliers basically have a take it or leave it attitude towards the terms of their agency agreements (which now all contain POPI requirements).	All parties are required to comply to the Act, this includes both private and public bodies, irrespective of their size. Complaints about unfair treatment can also be lodged with the Information Regulator directly, over and above other avenues that you have to raise concerns.

Can you then obtain consent up front from the client to quote on mulitple types of insurance products (life, invest, S/T)? even though they only requested a life quote at present?	Yes you can
How does POPI affect "in-app notifications", such as Discovery, Insurance Companies, etc. where the customer dowloaded the app. Does downloading the app give consent to the Company to send "in-app notifications" to the customer, and will an Opt Out in the T&C's be sufficient?	As long as the notification is aimed at all persons who have downloaded the app or on the website and not targeting specific clients, it si not regarded as in conflict. The opt-out must not be in the t&cs and must be easily accessible an d"exercisable" to the data subject
What would the Responsible Party's liability be if their IT service provider, who has access to their records, uses that data illegally?	The Responsible party will be subject to a possible investigation by the Information Regulator, and may also be sibject to Civil remedies under S99 of the Act. Furthermore S107 of the Act outlines penalities such as 12 months imprisonment, up to 10 yrs, R1m up to R10m or both. You therefore need to ensure that there is a contractual agreement in place between you and ANY operator that supplies you with services to ensure that they adhere to the ACt as well.
What about buying a book? - Will the seller by able to provide you with the information required to service those clients?	When you buy a book, the clients will all have to consent that te seller is allowed to provide you with the information. The FAIS Act also requires consnet before the info can be shared.
With regards to current contact lists / leads – my understanding is that provided the client has not opted out that you can continue communicating with them?	Where the person on the contact list is a client/has already been in contact with you regarding your services, then you will not need consent, but they must be able to opt out. Where a person is a non-client, then you need consent to electronic market to them. Phone calls are different, and you will not need consent in either case.
We currently ask exisitng clients to refer a collegue or family member (as a lead) - we ask for a name and a contact number. Are we still allowed to do this (obviously the lead given does not know that we are going to call or that his colleague has given us his information)?	The Act outlines (S18) the requirements when you do collect any PI from someone else - such as making sure that you advise the data subject where their information has been collected from, why it was collected, by whom it was collected, etc. It also requires that you provide the prospect Form 4 as prescribed by the Act when you want to market to them.
Within our brokerage , we use whatsapp groups with our staff. Clients information are made available on the groups. Some groups have the client added as a memeber of the group.	Remember that WhatsApp is typically handled on an individual's personal phone - any data subject's personal data would need to be managed by the person whose phone it is with due care and responsibility. The Information Regulator has expressed concern that the new privacy statement of WHatsApp is not aligned to the conditions of POPIA. We therefore advise that WhatsApp is used with care and contains minimal sensitive information - and rather use email as the formal communications tool. This may also be helpful when it comes to follow-up of queries in a formal channel.
What degree of responsibility does an OPERATOR have with regards to accuracy of information provided to them by the Resonsible Party?	They don't have any. The obligation rests with the responsible party ONLY to the extent that the operator is processing the information as per the responsible party's instruction. If the operator uses it for any other purpose the operator becomes the responsible party for the new purpose

We have been told that we can't keep an "Access list" when clients or visitors enter our premises (COVID related information) Is this true?	Under the Guidance note for the processing of PI under the Disaster Management Act you are still required to ensure you comply with POPIA - this implies that you can only keep those required records for the period that it is necessary to keep them for. IMportantly you may only use the information for purposes of contact tracing/management or preventing the spread of COVID. Below an extract: 4.5. Retention and restriction of records 4.5.1. Responsible parties must not retain records of personal information of data subjects for longer than authorised to achieve the purpose of detecting, containing and preventing the spread of COVID-19 unless such information is required for historical, statistical or research purposes and provided that adequate safeguards are in place. 4.5.2. A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record.
What about storing a client's cell phone number on your personal cell phone? Should you delete that phone number when the 5 year retention period (in terms of FAIS) is over?	POPIA doesn't apply to information for "purely household use". So where you have a personal phone and you are using that client's number for your own personal use and not for work purposes, then there is no need to delete after the 5 year period
If you have a list of Cancelled clients that you keep record of files deleted is the list not also counted or seen as record keeping that should also be destroyed?	This would be considered record-keeping and should be deleted in line with your retention periods.
I take it that destruction of paper can be done by the broker themselves instead of a service provider as long as they have a wriiten process on how it is actually destructed / destroyed?	That is correct
Does a request to delete information not potentially conflict with the FAIS / FICA requirements to keep records for a stipulated period of time?	You will only need to delete once the statutory retention periods have expired.
If someone voluntarily goes onto a company's website and downloads marketing material, is this regarded as direct marketing?	Yes, It will still be considered direct marketing - and the visitor must be advised of the conditions they are subject to when visiting the website as to what information is collected and processed.