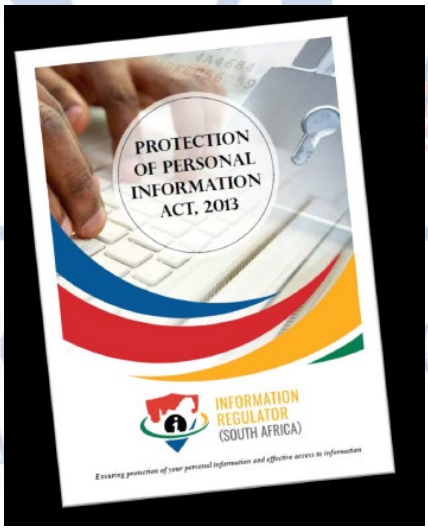
CMAC
HEALTHCARE CONSULTING
& FINANCIAL SERVICES
www.cmac.co.za
Financial Services Board: FSP 17112 and Council for Medical Schemes: ORG 35

RESERVE TRADING 10

CMAC
Motor, Household
& Business Insurance
Tel: (012) 991 0446 Email: shortterm@cmac.co.za
Gagemi Trade and Invest 107 (Pty) Ltd (2008/005811/07) T/A CMAC Short Term
Financial Services Board: FSP46176

POPIA implementation date

1 July 2021



These are the essential sections of the Act and pertain to –

- the conditions for 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.

General Code of Conduct (Board Notice 80 of 2003, as amended)

Section 3(2)(a):
A provider must have appropriate procedures and systems in place to store and retrieve such records and any other material documentation relating to the client or financial service rendered to the client and keep such client records and documentation safe from destruction.

Section 3(3):
A provider may not disclose any confidential information acquired or obtained from a client or a product supplier regarding such client or supplier, unless the written consent of the client or product supplier has been obtained beforehand or disclosure of the information is required in the public interest or under any law.

Section 11: A
Providers must always have and effectively employ the resources, procedures and appropriate technological systems that can reasonably be expected to eliminate as far as reasonably possible, the risk that clients, product suppliers and other providers or representatives will suffer financial loss through theft, fraud, other dishonest acts, poor administration, negligence, professional misconduct, or culpable omissions.

WHAT IS PERSONAL INFORMATION (PI)?

Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person.

SPECIAL PERSONAL INFORMATION

The processing of special personal information provides for a higher degree of protection, due to the sensitive nature of such information. Special personal information includes information concerning a **child** and personal information concerning **the religious or philosophical beliefs**, **race or ethnic origin**, **trade union membership**, **political persuasion**, **health, biometric information, sexual life or criminal behaviour** of a data subject.

Special rules apply to the processing of personal information of children.

PROCESSING OF PERSONAL INFORMATION OF CHILDREN

The POPI Act recognises that children are vulnerable. In terms of section 34 a responsible party may not process personal information concerning a child unless authorisation therefore is provided in the Act. The prohibition does not apply if the processing is –

- carried out with the prior consent of a competent person;
- necessary for the establishment, exercise or defence of a right or obligation in law or international public law;
- for historical, statistical or research purposes and if the purpose serves a public interest and the processing is necessary for the purpose concerned;
- of personal information which has deliberately been made public by the child, with the consent of a competent person.

''Child'' means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him or herself.
In certain circumstances legislation will render a child competent, like allowing a child to open a banking account at the age of 16. The processing of a child's personal information for this purpose would be regarded as being authorised in terms of legislation granting such right to the child. A competent person will assist the child in this case. Processing must be limited to what is reasonably necessary and the responsible party must establish procedures to protect the integrity and confidentiality of the personal information collected from children.

Important when processing personal information of a child:

- Obtain the prior consent of a competent person;
- Where a child's information is provided by a third party, obtain written confirmation that the prior consent of a competent person has been obtained;
- In all other instances, ensure that a child's information is deleted as soon as reasonably possible after its receipt, or if its processing is no longer necessary for the purposes of the business performing its function.

Responsible parties and their employees will be well advised to ensure compliance with the conditions for processing of special personal information in their businesses, especially that of children, and make special reference to such processing in their privacy policies.

WHAT IS PROCESSING?

Processing relates to the activity concerning PI and includes any operation or set of operations connected to that information. The Act lists the following actions as part of processing:

- Alteration
- Collation
- Collection
- Consultation
- Degradation
- Dissemination
- Distribution
- Erasure or destruction
- Merging
- Modification
- Organisation
- Receipt
- Recording
- Restriction
- Storage
- Updating
- Use
- Linking

This means that by possessing any such client information, be it in a hard copy or digital, makes you responsible in terms of the Act.

DATA PROTECTION PRINCIPLES

- PI must be processed fairly and lawfully; this includes being open and transparent.
- PI may not be processed unless one of the processing grounds exists.
- PI may only be processed if, given the purpose for which it is processed, it is adequate, relevant, and not excessive.
- PI must be collected for a specific, explicitly defined, and lawful purpose related to a function or activity of the responsible party.
- PI processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- PI shall not be further processed in any manner incompatible with the specified purposes.
- PI shall be accurate and, where necessary, kept up to date.

- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of PI and against accidental loss or destruction of, or damage to, PI.
- PI shall be processed in accordance with the rights of data subjects.
- PI shall not be transferred to a country unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

CONDITIONS 1 & 6: ACCOUNTABILITY, OPENNESS / TRANSPARENCY

- Accountability – you and your employees must comply with POPIA and all internal privacy policies.
- People is entitled to know:
    - who has their information;
    - what it will be used for;
    - the recipients or categories of recipients;
    - whether replies to any questions are obligatory or voluntary, as well the possible consequences of failure to reply;
    - the possibility of transfer to third parties; and
    - the right to access, to rectify and to oppose.
- These disclosures must typically be done before a person gives his/her data to a company to enable them to make an informed decision.
- Condensed disclosures and Privacy Notice

ACCOUNTABILITY CHECKLIST

- Have you determined who your Information Officer will be, as required by POPIA?
- Do your contracts with your IT providers and other service providers cater for the POPIA conditions?
- Do you have processes in place to verify that your service providers meet their contractual responsibilities with regards to POPIA?

OPENNESS CHECKLIST

- Do you inform clients when you collect their PI what the purpose is, as well as the consequence of not providing information?
- Do you keep evidence of the consent provided by prospects and clients for the collection and processing of their information?

CONDITION 2: PI MAY NOT BE PROCESSED UNLESS ONE OF THE PROCESSING GROUNDS EXISTS.

- Consent
    - informed (give data subjects information in a concise and clear manner on the purpose for processing)
    - freely given

- specific (consent should be obtained for specific purposes, the terminology used in the consent form should not be in general terms but must be specific having regard to the processing purpose)

- Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party
- Processing complies with an obligation imposed by law on the responsible party
- Processing protects a legitimate interest of the data subject
- Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied

PROCESS LIMITATION CHECKLIST

- Does your on boarding and fact-finding documentation include consent from prospects/clients to process their PI?
- Do you collect PI using third parties?
- If so, are your prospects/clients aware that you are collecting their information, and have they given consent?
- Does your client documentation explain to clients that you will process their PI, subject to the requirements of POPIA and other legislation?
- Do you only collect data that is relevant to the purpose you are collecting data for?
- Do you give clients the option to opt out from any newsletters or campaigns that you run in your practice?

CONDITION 3: PURPOSE SPECIFICATION

- You may only process personal information for the purposes disclosed to customers.
- Purposes must be specific, explicitly defined, and lawful
- Examples of purposes:

- to offer clients ongoing financial services
- to provide clients with information about products or services that are deemed suitable to their financial needs
- underwriting
- assessment and processing of claims
- credit searches and/or verification
- claims checks (Industry Life & Claims Registers)
- fraud prevention and detection
- market research and statistical analysis
- audit & record keeping purposes
- to comply with legal & regulatory requirements
- verifying clients' identity
- sharing with service providers who process information on your behalf or who render a service to you

PURPOSE SPECIFICATION CHECKLIST

- Does your client documentation explain the purpose for which data is collected?
- Does your client documentation explain how long data will be kept (e.g., to the FAIS requirements)?

CONDITION 3: RETENTION AND DESTRUCTION

- PI processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Exemptions
- Retention of the record is required or authorised by law
- The responsible party reasonably requires the record for lawful purposes related to its functions or activities
- Retention of the record is required by a contract between the parties thereto
- The data subject or a competent person where the data subject is a child has consented to the retention of the record

CONDITION 4: FURTHER PROCESSING

Personal information may not be used for any purpose other than that for which it was collected.

FURTHER PROCESSING LIMITATION CHECKLIST

- Do you do any further processing of client PI?
- Have you determined for yourself that the further processing is in line with the purpose for which the PI was collected in the first instance?
- If the further processing is not in line with the purpose for which the PI was obtained initially, do you have any legal justification (e.g., the data subject's consent) to do the further processing?
- Is PI transferred to other countries, e.g., if your data is hosted offshore in the cloud?
- Do you ensure that this information is protected adequately by law, corporate rule, or binding agreement?

CONDITION 5: INFORMATION QUALITY

You must take reasonable steps to keep personal information complete, accurate, updated and not misleading, regard being had to the purpose for which the information was collected or processed.

INFORMATION QUALITY CHECKLIST

- Do you inform clients of the importance of providing complete and accurate information, and that they should inform you if data is incorrect or changes over time?
- Do you review and update client information on a regular basis, e.g., when you review their financial plans?

CONDITION 7 – INFORMATION SECURITY

- The risk of data loss and subsequent fraud:
- an increase of financial crime because poor controls over customer data present opportunities for thieves and fraudsters to steal data and commit identity fraud and other financial crime;
- consumer protection at risk because data loss, especially on a large scale, could cause significant detriment to individuals;
- market confidence could be affected by large data loss which causes consumers to question the integrity or safety of the financial sector or service delivery channels, such as online banking.

- Firms do not understand the value to criminals of customer data.
- Generally, firms are only concerned about data security risk if there is some risk to their own business – they are not concerned about protecting their customers from wider identity theft.
- Safekeeping of customer data is a crucial responsibility for firms.
- The secure handling of customer data is also part of the 'Treating Customers Fairly' standard that all firms must adhere to.

CONDITION 7 – INFORMATION SECURITY … WHAT DOES POPIA SAY

- **A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent:**
- loss of, damage to or unauthorised destruction of personal information; and
- unlawful access to or processing of personal information.
- **To give effect to this, the responsible party must take reasonable measures to:**
- identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are effectively implemented; and
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
- Have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

GOOD BUSINESS PRACTICE FOR SECURITY

- Customer data taken offsite on laptops or other portable devices must be encrypted.
- Secure transmission of data – emails, cd's, post, DropBox, memory sticks, fax to email
- Access management
  - Least privilege access
  - Employees who move or leave
- Strong passwords
- Back-up data
  - Secure transmission by encryption
  - Secure storage
- Email and internet access
- Proper asset management
- Wipe laptops before re-distributing

GOOD BUSINESS PRACTISES FOR SECURITY . . . IT'S NOT ALL ABOUT IT

- Data losses – know about it and respond to it
- Consider notification to regulator and data subjects
- Physical security – for the building and in the building
- Proper vetting of staff
  - upfront and ongoing
  - permanent and temporary
  - ensure that employment agencies also do proper vetting
- Lock filing cabinets
- Clean desk policy
- Collect faxes and printouts immediately
- Disposal of paper containing personal data – shredding
- Policies, procedures, and guidelines
- Training and awareness
  - Many instances of data loss occur because staff do not know or understand relevant policies and procedures. So, it is good practice for senior management to put in place appropriate training and awareness mechanisms to ensure that their staff understand the relevance of policies and procedures to their roles.
  - It is not realistic to expect staff to read and act on policies simply because they are available on the firm's intranet or in an employee handbook.

SECURITY SAFEGUARDS

- Is all PI of clients and staff in your practice stored securely, with regard to both paper and electronic versions?
- If you keep paper, is it locked away?
- Do you have a clean desk policy?
- Do you shred all paper before disposing of it?
- Have you considered scanning the information and only keeping electronic versions?

- Do you manage the access to electronic information, by your staff and any operator acting on your behalf?
- Are all devices, including computers, storage devices and servers, in your practice properly protected, e.g., with passwords, anti-virus software, encryption?
- Do your employee contracts include the responsibilities of your staff about meeting POPIA conditions?
- Are your staff all made aware of the legal requirements about protecting PI?
- Does their training include detail on their specific responsibilities?
- Do you revoke the access of staff members when they leave your service, both to applications used in your practice and product provider applications?
- Do you keep record of prospects that you have contacted who did not give you consent for further interaction, so that you do not contact them again?
- Do you have processes in place to ensure their data is not used for any other purpose?
- Do you verify the identity of clients when you receive a request for information, to ensure that information is provided to the correct person?
- What processes do you have in place to prevent PI from falling into the wrong hands?
- Do you have a process to detect and report security breaches to the Information Regulator and clients or staff whose PI is impacted?

Condition 7: OPERATORS

- Someone who processes PI on your behalf
- Printers and mailing companies
- Marketing companies
- Providers of off-site storage facilities for archived files and back-up tapes
- Confidential waste disposal specialists
- They may only do so with your authorization and knowledge
- They must treat all PI as confidential
- You must have a written contract with them that contains the necessary data protection clauses
- They must maintain the same level of protection of the PI that you would have afforded the PI
- They must notify you when there has been an information security breach
- Outsourcing
- choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures they take
- ensure compliance with those measures, and
- ensure the data processor carried out the processing under a contract containing certain terms and conditions.

Condition 7: OTHER THIRD PARTIES (we are still with security)

- Third party suppliers that have access to data
- Examples of the types of third parties used by the firms who have direct or indirect access to customer data include:
- couriers;
- IT contractors and IT maintenance companies;

- cleaners;
- security;
- catering staff; and
- staff from other companies where offices and buildings are shared.

➢ Essential that firms are fully aware of the additional data security risks that arise from allowing third parties to access their customer data.
➢ Good practice for firms to ensure that any individual or company with access to their customer data has appropriate data security standards.

CONDITION 8: DATA SUBJECT PARTICIPATION

➢ Right to know that their information is processed and what it will be used for
➢ Right of access
➢ Right to object
➢ Right to ask for correction
➢ Right to ask for deletion
➢ Right to complain to Regulator and civil courts

DATA SUBJECT PARTICIPATION CHECKLIST

➢ Do you inform clients about their rights to access and ask for correction or deletion of information?
➢ Do you keep record of any third party you provided PI to?
➢ Do you have a process to retrieve the necessary information on request?

CONSENT MUST BE OBTAINED TO COMMUNICATE TO PROSPECTIVE CUSTOMERS

While best practice email and SMS marketing has always worked this way, the law now compels us to do so. It is now against the law to use direct marketing tactics to sell to a prospective customer without their consent.
You may however contact a recipient **once**, to obtain this consent (an opt-in campaign) and if they do not explicitly provide you with consent all future communications must cease. Once a recipient opts-in, a method of unsubscribing must be provided as is the current standard practice.

DIRECT MARKETING TO CUSTOMERS

Direct marketing to customers is permitted under POPI without having to get their explicit consent. All other rules still apply through, including being able to only market similar products or services to them.

GENERAL CONSENT VS SPECIFIC CONSENT

Under POPI you will need to get consent for the direct marketing of specific products / services or ranges of products / services. You may not market other unrelated products / services. For example, if a prospect opts in to receive travel deals, you cannot market beer to them. Provide a detailed description of what information subscribers will receive on your subscription web-form to avoid any confusion.

TRANSPARENCY OF THE SENDER

All communications must include the identity and contact details of the sender. Ensure that your company information is a standard part of every email you send.
It is also good practice to ensure that your email footer has a complaints link to provide recipients with an option to complain to you if they feel a violation of their privacy has occurred. It is better to receive these complaints and deal with them directly rather than to be reported to the authorities.

PAIA – PROMOTION OF ACCESS TO INFORMATION ACT
Compiled in accordance of Section 51 of the Act

The Promotion of Access to information Act, 2000, PAIA gives effect to section 32 of the Constitution, which provides that everyone has the right to access information held by the State, as well as information held by another person (or private body) when such privately held information is required to exercise a right or to protect a right.

PAIA, provides that a person requesting information must be given access to any record of a private body, if that record is required for the exercise or the protection of a right. However, such request has to comply with the procedural requirements laid down by the Act.

MANUAL ATTACHED
VERY IMPORTANT:

1. PROCEDURE FOR OBTAINING ACCESS TO INFORMATION

Any person who wishes to request any information held by the FSP to exercise a right may contact the FSP's information officer at the FSP's contact details.

A request for access to information must be made in the prescribed form to the information officer indicated.

Once the "Request for Information Form" has been submitted, the information officer will notify the person who submitted the request of the prescribed fee (if any) payable before further processing the request.

A fee may be charged for access to any records. If the request is granted, the person who submitted the request will be accordingly notified and a further fee may be payable. The additional fee would be for the reproduction, preparation and time reasonably required to search for and preparation of the information.

An individual seeking access to a record containing their own personal information will not be charged a request fee.

A person submitting the request must:

- indicate the identity of the person seeking access to the information
- provide sufficient particulars to enable the information officer to identify the information requested
- specify the format in which the information is required
- indicate the contact details of the person requiring the information
- indicate the right to be exercised and/or to be protected and specify the reasons why the information required will enable the person to protect and/or exercise the right
- where the person requesting the information wishes to be informed of the decision of the request in a particular manner, state the manner and particulars to be so informed
- if the request for information is made on behalf of another person, submit proof that the person submitting the request, has obtained the necessary authorisation to do so.

2. GROUNDS FOR REFUSAL OF ACCESS TO RECORDS

The Promotion of Access to information Act provides several grounds on which a request for access to information must be refused. These grounds mainly concern instances where the privacy and interest of other individuals are protected, where such records are already otherwise publicly available, instances where public interest are not saved, the mandatory protection of commercial information of commercial information of a third party, as well as the mandatory protection of certain confidential information of a third party.

CATEGORISATION OF COMPLAINTS

Legislation (as pointed out above) currently requires FSP's to categories complaints in prescribed ways. Categorisation of complaints is part of a complaints management framework. This will enable employees, operators, and others to identify when there is privacy complaint and allow for a timeous escalation of the complaint to the Information Officer.

In order to identify a privacy complaint, the following questions can be asked, following which a complaint can be categorised and then managed as a privacy complaint (this is not an exhaustive list)

- The complainant has said that this is a complaint or request in terms of the Protection of Personal Information Act or the Promotion of Access to Information Act or has sent us a prescribed form under POPIA or PAIA.
- The complainant wants to know whether and what personal information we hold about him/her/their child or who has access to it.
- The complainant says we have accessed someone's personal information unlawfully.

- The complainant has threatened to complain, or has complained, about us or our operators to the Information Regulator.
- The complainant has said that a service provider's data subject's personal information has been accessed or acquired by a person not authorised to have it.
- The complainant has said that a service provider's data subject's personal information is not being kept securely or confidentially by us.
- The complaint is about us or our operator direct marketing to someone without consent.
- The complainant has said that we or our operators are collecting or processing someone's personal information in an unlawful, unauthorised or incorrect way or without their consent.
- The complainant wants us or our operators to stop processing his/her/their child's personal information.
- The complainant's complaint relates to us or our operators deleting or destroying personal information we hold about him/her/their child.
- The complainant's complaint relates to personal information we or our operators hold about him/her/their child or requiring correction or being inaccurate, misleading, incomplete, or needing updating.

INFORMATION OFFICER DUTIES AND RESPONSIBILITIES

The POPI Act (POPIA) stipulates that each business must appoint an Information Officer, and where necessary, one or more Deputy Information Officers, depending on the size, nature, and complexity of the business. The Information Officer must ensure that the business complies with the provisions of POPIA and of the Promotion of Access to Information Act (PAIA).

It is important to note that the responsible party, being the person that determines the purpose of and means for processing personal information, remains ultimately responsible for ensuring that the processing of personal information is done in a lawful manner.

Information Officer duties and responsibilities:

In terms of section 55 (1) of POPIA, an Information Officer's responsibilities include:

a) The **encouragement of compliance** with the eight conditions for the lawful processing of personal information;

b) Dealing with requests made in terms of this Act, for example:
p**roviding assistance, free of charge**, to enable a requester or data subject to comply with processes for submitting a request in terms of PAIA and POPIA;
assisting a requester or data subject that has made any request that does not comply with the requirements of PAIA or POPIA, and **providing any information that would assist in making the request in the prescribed form.**

c) **Working with the Regulator** in relation to investigations conducted in respect of the responsible party, for example:
A responsible party must obtain prior authorisation from the Regulator for processing of any unique identifiers of data subjects;
processing of information on criminal behaviour or on unlawful conduct on behalf of

third parties;

- processing of information for the purposes of credit reporting; and
- transferring of special personal information or the personal information of children to a third party in a foreign country.

The responsible party is prohibited from carrying out processing of information until completion of the investigation or until notice has been given that a more detailed investigation will not be conducted.

Failure to notify the Regulator of the processing listed above is an offence and upon conviction, the responsible party will be liable to a fine or imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment.

d) Ensuring compliance by the body with other provisions of this Act, for example:
POPIA prescribes eight conditions for the lawful processing of personal information by or for a responsible party, and it is the responsibility of an Information Officer to ensure compliance with those conditions;

e) As may otherwise be prescribed by the Regulator.

In terms of regulation 4 of the POPI Regulations, Information Officers must, in addition to the responsibilities referred to in section 55(1) of POPIA above, ensure that:

- A compliance framework is developed, implemented, monitored and maintained;
- An impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
- A manual is developed, monitored, maintained and made available as prescribed in terms of PAIA. The manual must specify – • the purpose of the processing of personal information;
- a description of the categories of data subjects and of the information or categories
- of information relating thereto;
- the recipients to whom the personal information may be supplied;
- any contemplated cross-border flows of personal information; and
- an assessment of information security measures to be implemented and monitored by the responsible party
- The manual must be available on the website and at the office or offices of the responsible party for public inspection.
- Internal measures and systems are developed to process requests for information or access thereto; and
- Internal awareness and training sessions are conducted regarding the provisions of the Act, regulations, codes of conduct, or information obtained from the Regulator.

Contact Us
For questions regarding our CMAC POPIA Manual, contact CMAC at: info@cmac.co.za

Disclaimer: *This Website and its attachments and any rights attached thereto, are the property of CMAC (Care Medical Aid Consultants). It is private and confidential, and subject to legal privilege attended for this site only. CMAC does not warrant that this site is free of errors, interception, or interferences. If this site and its content constitute spam, contains infringing or offensive content, or used for purposes unrelated to the official business of CMAC, CMAC shall not be liable for any loss, damage or expense of whatever nature resulting therefrom. Any use, printing, storage, disclosure, copying or taking of any action in reliance of the contents on this site is prohibited and may be unlawful.*