TECHNOLOGY, MEDIA & TELECOMMUNICATIONS SECTOR

CDH
CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA

POPIA COMPLIANCE CHECKLIST

Compiled by Lucinde Rhoodie, Kara Meiring, Ngeti Dlamini and Preeta Bhagattjee

8 APRIL 2021

The operative provisions of the Protection of Personal Information Act 4 of 2013 (POPIA) came into effect on 1 July 2020, with a grace period of a year in which companies must ensure that they are compliant. Companies must ensure that their business practices and the way they interact with customers, clients or consumers adhere to the requisite privacy laws, as well as confirming that the way they collect, store or process their employees' information aligns with the protections set out in POPIA.

The below table contains a useful generic checklist that businesses can use to ensure that they are POPIA compliant by 1 July 2021.

CDH's POPIA compliance checklist seeks to assist businesses (noting that POPIA applies to both public and private bodies) with a general heat map to check its compliance levels and areas of risk relating to POPIA compliance and has merely been provided to assist in expediting the POPIA compliance process.

The checklist does not make provision for every eventuality and serves only as a useful guide to assist businesses to start focusing on the most common instances where businesses need to be POPIA compliant. The checklist should in no way to be construed as a substitute for seeking legal advice to ensure that your business is fully compliant with the requirements of POPIA.

GENERIC POPIA COMPLIANCE CHECKLIST:

PART A: PRELIMINARY STEPS

STEP	DESCRIPTION	STATUS

1. Appoint an Information Officer and deputy information officers, where required	• **Register your Information Officer and deputy information officers with the Information Regulator on their electronic portal. The Information Regulator has issued a Guidance Note on 1 April 2021 describing the registration process for each legal entity who is considered a responsible party to register their information officer and deputy information officers.**
	• **Set out the Information Officer's general responsibilities namely:**
	  • encouraging and ensuring the business' compliance with POPIA;
	  • dealing with information access requests pursuant to POPIA; and
	  • working with the Information Regulator in relation to investigations conducted in terms of POPIA.
	• **The Information Officer are to ensure that they comply with the prescribed responsibilities, ensuring that:**
	  • a compliance framework is developed, implemented, monitored and maintained;
	  • a personal information 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 PAIA manual is put in place or updated, as prescribed in sections 14 and 51 of POPIA;
	  • internal measures are developed together with adequate systems to process requests for information or access thereto; and
	  • internal awareness sessions are conducted regarding the provisions of POPIA, regulations made in terms of POPIA, codes of conduct, or information obtained from the Regulator.	

POPIA COMPLIANCE CHECKLIST

Compiled by Lucinde Rhoodie, Kara Meiring, Ngeti Dlamini and Preeta Bhagattjee

PART A: PRELIMINARY STEPS*...continued*

STEP	DESCRIPTION	STATUS

2. Assess current records of personal information	• **Assess and compile a list of the personal information you currently process in your business (see definition schedule for information that will be classified as *"personal information"*.)**
	• **Assess and compile a list of any special personal information that is processed in your business. Special personal information relates to:**
	  • the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of the data subject; or
	  • the criminal behaviour of a data subject to the extent that such information relates to (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.	

3. Audit current process used to process personal information (collect/record/ store and disseminate data)	• **Evaluate the current processing activities that are being undertaken by the business involving personal information and/or special personal information.**
	• **Create a detailed list/schedule of these processing activities setting out:**
	  • where the information is being processed;
	  • what type of information is being processed; and
	  • by whom the information is being processed.
	• **Evaluate all service agreements relating to data processing and update your contracts accordingly.**	

4. Ensure appropriate security safeguards are in place	• **Secure the integrity and confidentiality of personal information in your possession or under your 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.
	• **Take reasonable measures to:**
	  • identify internal and external risks;
	  • establish and maintain safeguards against the identified risks;
	  • regularly verify that the safeguards are implemented effectively; and
	  • ensure that the safeguards are continuously updated.	

PART B: DEALING WITH INFORMATION IN YOUR POSSESSION

STEP	DESCRIPTION	STATUS

1. Verify the quality of the information	• **Take reasonable steps to ensure that personal information is:**
	  • complete;
	  • accurate;
	  • not misleading; and
	  • updated.	

2. Further processing	• **Check the rationale for any further processing of personal information and whether it is in line with the initial purpose for which it was collected.** • **If information has been received via a third party for further processing, ensure that the further processing is compatible with the purpose for which the data was initially collected.**	

POPIA COMPLIANCE CHECKLIST

Compiled by Lucinde Rhoodie, Kara Meiring, Ngeti Dlamini and Preeta Bhagattjee

PART B: DEALING WITH INFORMATION IN YOUR POSSESSION *...continued*

STEP	DESCRIPTION	STATUS

3. Monitor and manage your retention of records and disposal thereof	• **Ensure that records of personal information are not retained any longer than is necessary for achieving the purpose for which the information was collected.**
	• **If personal information is retained for a longer period, check whether any of the following exceptions apply:**
	  • retention of the record is required or authorised by law;
	  • you reasonably require the record for lawful purposes related to your functions or activities;
	  • retention of the record is required in terms of a contract between parties thereto; or
	  • the data subject has consented to the retention of the record.
	• **Confirm whether records of personal information fall within the category of serving historical, statistical or research purposes.**
	• **Ensure that you establish appropriate safeguards against the records being used for any other purpose.**	

4. Delete unauthorised information	• **Delete any record of personal information or de-identify it (see definitions list) as soon as reasonably practicable after you are no longer authorised to retain such information.**
	• **You will no longer be authorised to retain information if:**
	  • The information is no longer necessary for the purpose for which it was obtained;
	  • The data subject has withdrawn their consent for the processing of their information;
	  • The data subject has validly objected to the processing or further processing of their information; or
	  • The data subject has made a valid request for the deletion of their personal information.	

PART C: OBTAINING AND PROCESSING INFORMATION

STEP	DESCRIPTION	STATUS
1. Define the purpose of the information gathering/ processing	• **Ensure that the personal information that you intend to collect is for a specific, explicitly defined, and lawful purpose that relates to a function or activity of your company.** • **Determine the duration for which the information will be retained in order to achieve this purpose.**	

2. Notify the data subject	• **Take the necessary steps to notify the person whose information is being processed.**
	• **Inform them of:**
	  • what information is being processed;
	  • why their information is being processed;
	  • your company name and address;
	  • whether the provision of the information is voluntary or mandatory;
	  • the consequences of failure to provide the information;
	  • any particular law authorising or requiring the collection of information;
	  • whether the information will be transferred to a third party or foreign country; and
	  • if the information is not collected from them directly, the source from which it is collected.	

POPIA COMPLIANCE CHECKLIST

Compiled by Lucinde Rhoodie, Kara Meiring, Ngeti Dlamini and Preeta Bhagattjee

PART C: OBTAINING AND PROCESSING INFORMATION *...continued*

STEP	DESCRIPTION	STATUS

3. Determine the legal basis for processing of personal information	• Assess and ensure that you have a legal basis (in terms of POPIA) for each processing activity which you undertake.
	• Ensure that you obtain the informed consent of the data subject (or in the case of a child, a competent person) in order to obtain and process their information, where this may be required.
	• The general legal bases provided under POPIA, apart from consent, include:
	  • the processing of the personal information is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;
	  • the processing complies with an obligation imposed on you by law;
	  • the processing protects a legitimate interest of the data subject; or
	  • the processing of the personal information is necessary for pursuing the legitimate interests of your company or of a third party to whom the information is supplied.
	• Please note that there are specific requirements relating to the different types of special personal information.	

PART D: REQUESTS FOR ACCESS, CORRECTION AND/OR DELETION

STEP	DESCRIPTION	STATUS

1. Create an easy process for the receipt of DATA SUBJECT ACCESS requests	• Set up a mechanism (included in your PAIA manual and privacy policy) whereby data subjects can:
	  • inquire whether you hold their personal information;
	  • request the identity of all third parties with access to their information; and
	  • request a record or description of their personal information.
	• Establish an accessible process to allow a data subject to:
	  • make corrections to information;
	  • withdraw consent for the processing of information; and
	  • object to the collection of information.
	• Inform data subjects of their right to submit a complaint to the Information Regulator.	

2. Action the request	• If a request to correct, delete or destroy a record of personal information been received from the data subject, ensure that where applicable:
	  • the information has been corrected;
	  • the information has been destroyed or deleted;
	  • credible evidence has been provided to the data subject's satisfaction in support of the information; or
	  • where agreement cannot be reached and the data subject so requests, take reasonable steps to attach a note to the information, which states that a correction of the information has been requested, but that the correction has not been made.	

3. Inform the relevant parties	• Inform the data subject of the action taken pursuant to their request for deletion/correction. • If the correction, destruction or deletion of information has an impact on decisions made by persons in your company, ensure that each person to whom the information was divulged, where reasonably practical, has been informed of such correction, destruction or deletion.	

POPIA COMPLIANCE CHECKLIST

Compiled by Lucinde Rhoodie, Kara Meiring, Ngeti Dlamini and Preeta Bhagattjee

PART E: DIRECT MARKETING

STEP	DESCRIPTION	STATUS

1. Classify the data subject	If you engage in direct marketing (via electronic means):
	• Determine in which category a data subject falls, i.e.:
	  • have they given their consent for the processing of their information (for the purpose of direct marketing); or
	  • are they already a customer of your company.	

2. Obtain consent in the prescribed manner and form	• Approach a data subject who has not yet given their consent if:
	  • their consent is required (i.e. they are not a customer); and
	  • they have not previously withheld their consent.
	• Keep a record of the data subjects that you have approached, as you may only approach a data subject once.	

3. Comply with specific processing requirements	• Ensure that the customer information has been obtained:
	  • in the context of the sale of a product or service; and
	  • for the purpose of direct marketing of your own products or services.
	• Give the data subject a reasonable opportunity to freely and informally object to the use of their electronic details at the time of obtaining their details and every time communication is sent to them.
	• Check that all direct marketing communications contain:
	  • details of the identity of the sender; and
	  • an address or contact details to which the data subject can object to receiving such information in future.	

PART F: CROSS-BORDER TRANSFERS

STEP	DESCRIPTION	STATUS

1. Comply with additional requirements	• Take steps to determine whether you are entitled to transfer personal information about a data subject to athird party in a foreign country.
	• Confirm that at least one of the additional requirements have been met:
	  • the third party is subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection of personal information;
	  • the data subject consented to the transfer of the personal information to the third party in a foreign country;
	  • the transfer is necessary for the performance of a contract between the data subject and your company, or for the implementation of pre-contractual measures taken in respect of a request by the data subject;
	  • the transfer is necessary for the conclusion or performance of a contract concluded between your company and the third party in the interests of the data subject; or
	  • the transfer is for the benefit of the data subject and it is not reasonably practical to obtain the consent of the data subject to that transfer and if it were practical, the data subject would have provided their consent.	

POPIA COMPLIANCE CHECKLIST

Compiled by Lucinde Rhoodie, Kara Meiring, Ngeti Dlamini and Preeta Bhagattjee

LIST OF USEFUL DEFINITIONS:

"consent"	• **means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.**
"data subject"	• **means the person to whom personal information relates.**
"de-identify"	• **means, in relation to personal information of a data subject, to delete any information that:** • identifies the data subject; • can be used or manipulated by a reasonably foreseeable method to identify the data subject; or • can be linked by a reasonably foreseeable method to other information that identifies the data subject; and • "de-identified" has a corresponding meaning.
"direct marketing"	• **means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:** • promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or • requesting the data subject to make a donation of any kind for any reason.
"electronic communication"	• **means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.**
"operator"	• **means a person who processes personal information for the responsible party in terms of a contract or mandate, without coming under the direct authority of that party.**
"person"	• **means a natural or juristic person.**
"personal information"	• **means 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, email 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; and • the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
"private body"	• **means:** • a natural person who carries or has carried on any trade, business or profession, but only in such capacity; • a partnership which carries or has carried on any trade, business or profession; or • any former or existing juristic person, but excludes a public body.
"processing"	• **means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:** • the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; • dissemination by means of transmission, distribution or making available in any other form; or • merging, linking, as well as restriction, degradation, erasure or destruction of information.

POPIA COMPLIANCE CHECKLIST

Compiled by Lucinde Rhoodie, Kara Meiring, Ngeti Dlamini and Preeta Bhagattjee

LIST OF USEFUL DEFINITIONS:

"public body"	• **means:** • any department of state or administration in the national or provincial sphere of government; or • any other functionary of institution when: - exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or - exercising a public power or performing a public function in terms of any legislation.
"public record"	• **means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.**
"record"	• **means any recorded information:** • regardless of form or medium, including any of the following: • writing on any material; • information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; • label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; • book, map, plan, graph or drawing; • photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; • in the possession or under the control of the responsible party; • whether or not it was created by the responsible party; and • regardless of when it came into existence.
"Regulator"	• **means the Information Regulator established in terms of the Protection of Personal Information Act.**
"re-identify"	• **means, in relation to personal information of a data subject, to resurrect any information that has been de-identified, that:** • identifies the data subject; • can be used or manipulated by a reasonably foreseeable method to identify the data subject; or • can be linked by a reasonably foreseeable method to other information that identifies the data subject; • and "re-identified" has a corresponding meaning.
"responsible party"	• **means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.**
"special personal information"	• **means personal information relating to:** • the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of the data subject; or • the criminal behaviour of a data subject to the extent that such information relates to: - the alleged commission by a data subject of any offence; or - any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
"unique identifiers"	• **means any identifier that is assigned to a data subject and is used by the responsible party for the purposes of the operations of the responsible party and that uniquely identifies that data subject in relation to the responsible party.**

Please contact us at popia@cdhlegal.com should you require information on our customised and comprehensive compliance toolkits tailored specifically for application in different types of businesses.

CDH
CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA