Cp7

Complex Patrols Pty Ltd trading as Complex Patrols
Company Reg: **2017/381410/07** VAT Reg: **4460263207**
Postal Address: Post Net Suite 229, Private bag X3 Bloubergrant 7443
Address: 25 Northumberland Close, Parklands, 7441
Telephone: 021- 556 8089. Fax: 086 585 8016
Email: barry@complexpatrols.co.za opsmanager@complexpatrols.co.za
Registered as a security service provider by the Private Security Industry Regulatory Authority
Registration number 2111242

COMPLEX PATROLS PTY LTD GROUP

No.4 of 2013

PROTECTION OF PERSONAL INFORMATION ACT, 2013

COMPLIANCE MANUAL

CP/111111/2021

Background

Introduction

Background

Complex Patrols Pty Ltd (hereinafter referred to as Complex Patrols) opened for business in November 2011 and rapidly established itself as a leader in the security industry, particularly in the Greater Blouberg area and is today a household name and a trusted security service provider. Complex Patrols is a PSIRA registered and authorised security service provider that renders Armed response and alarm monitoring, technical security product installations as well as an enforcement agency for Body Corporate rules.

Our clients are our most valued assets, so it goes without saying that protecting our client's personal information is especially important to us and this has always been strictly enforced.

With the Protection of Private Information act 4 of 2013 (POPIA) having full effect from the 1st of July 2021, preparations for full compliance thereto have been ongoing and except for a few minor changes in how we protect information, it has largely been about appointing and registering our Information Officer, compiling documents required by the act, crossing all the T's, and dotting the I's.

Complex Patrols welcomes the Protection of Personal Information act of 2013 and are committed to full compliance thereto.

Introduction

The act is to give effect to, and the Information Regulator is tasked with, the protection, promoting, and ensuring an equilibrium between:

a. Individual constitutional rights to the protection of, privacy and personal information

b. the need for public access to information for the purpose of conducting business.

c. regulate the way personal information may be processed.

This protection of private information compliance manual has been compiled with the aim of ensuring compliance by setting out the basis for processing(using) personal information obtained from our clients either, manually and or automated, this may include any stage from collecting to destruction thereof.

A. Complex Patrols obligations to our clients, we will only collect personal information when necessary and only what is legally required, this is done by means of a service contract agreement, electronic sources such as, Complex Patrols website, emails, WhatsApp, Telegram, SMSs, and Google ads, for the purposes of (1) satisfying any legal requirement to do so and (2) to fulfill contractual obligations in rendering our services effectively and efficiently to our clients.

We will ensure:

1.1 *Accountability*; we will follow POPI at all applicable times and ensure that we process personal information legally and reasonably, so as not to arbitrarily infringe on the privacy of our clients.

1.2 *Processing limitations*; we will process information as agreed with our client and only for the *purposes specific*,

1.2.1) to which it is intended.

1.2.2) to enable us to render our service.

1.2.3) to enable us to collect revenue due for services rendered.

1.3 *To obtain consent to process,* personal information where necessary **(See CP2 consent)**

1.3.1) *Where consent is not requested*, the processing of the client's personal information will be to protect a legitimate interest that requires protection because of a legal obligation thereto.

1.4 *Minimally*: To only collect the absolute minimal information required from the client

1.5 *Data subject participation*, collect the personal information we require directly from the client, unless:

1.5.1) the information is a matter of public record,

1.5.2) the client has agreed to the collection of their personal information from another.

source

1.5.3) the collection of the information from another source does not prejudice the client.

1.5.4) the information to be collected is necessary for the maintenance of law and order.

1.5.5) the information to be collected is necessary for national security.

1.5.6) the information to be collected is to comply with a legal obligation.

1.5.7) the information to be collected is necessary for an obligation to SARS.

1.5.8) the information collected elsewhere is required for the conduct of proceedings in any court or tribunal, where these proceedings have commenced or are reasonably contemplated.

1.5.9) Further information is required to maintain our legitimate interests.

1.5.10) where requesting consent would influence the purpose of the collection of the information.

1.5.11) requesting consent is not reasonably practical.

1.6 That the personal information which we collect and process, is minimal in nature, is not misleading, is complete, is accurate and is current.

1.7. *Data retention*:

17.1) We retain records of the personal information we have collected for the minimum period as required by law unless the client has given their consent or has directed us to retain the records for longer.

1.8 *Data destruction:*

18.1) We destroy or delete records of the personal information for the purpose of de-identifying the client as soon as reasonably possible or after the time for which we were obligated to hold the records have expired.

18.2) **Where there is no response to any of our quotations on record, personal information obtained at quotation level, will be deleted/destroyed after 90 days from the date the quotation was first sent to the client)**

1.9. *Further data processing limitation:*

Stop the processing of personal information where:

1.9.1) the accuracy of the information is contested, only for the period needed to enable us to confirm the accuracy of the information.

1.9.2) the purpose for which the personal information was collected has been achieved and is being retained only for the purposes of proof.

1.9.4) the client requests that the personal information not be destroyed or deleted, but rather retained.

1.9.5) the required consent is withdrawn, or if a valid objection is raised.

2. Continue to process personal information:

2.1 only if required and not further prevented to as per the above relevant paragraphs.

2.2 where further processing is necessary because of a threat to public health or public safety or to the life or health of a client, or a third person.

2.3 where this is required by the Information Regulator appointed in terms of POPI.

2.4 where necessary to recover revenue due to Complex Patrols for services rendered and or for the recovery of equipment being the legal property of Complex Patrols.

B. Complex Patrols Client rights

1. *Openness*, notify our clients of the purpose of the collection of the personal information.
2. Advise our clients of our duty to them in terms of POPI by way of such information included in our contract/s and or via email prior to or on presentation of any quotation **(see cp1 client notice)**
3. In cases where the client's consent is required and obtained to process their personal information, this consent may be withdrawn by the client, subject to, such withdrawal not placing the client in breach of any contract with Complex Patrols.
4. Should the withdrawal as per clause 2 above occur and the client desires further services from Complex Patrols, a new completed consent form must be obtained from the client **(See CP2 consent).**
5. In cases where we process personal information without consent to protect a legitimate interest or to comply with the law or to pursue or to protect, our legitimate interests, the client has the right to object to such processing. **(See cp4 {form 1 of the regulations})**
6. All clients are entitled to lodge a complaint regarding our application of the POPI act with the Information Regulator. **(See page 14 hereof)**

C. Security measures to protect personal information.

1. To secure the integrity and confidentiality of the personal information of any person in the possession of Complex Patrols and to protect information against loss or damage or unauthorised access, we have implemented and will continue to maintain the following security measures.

Security safeguards:

1.1) Retain the physical file and the electronic data related to the processing of the personal information in a safe and secure environment until deleted/destroyed/de-identified or returned, or unless the continued retention thereof is a legal obligation, including any obligation to SARS.

1.2) Take special care with our client's bank account details. We further acknowledge that we are not entitled to obtain or disclose or solicit the disclosure of such banking details unless we have the client's specific consent.

1.3) Our business premises where records are kept will always remain protected by Access control, CCTV monitoring, 24-hour PSIRA registered Security officer presence and Armed response. In addition, any request for any file containing personal information for the purposes of conducting ordinary business will require the staff member to record such in a register for tracking and accountability purposes by booking out and booking in on return.

1.4) Any file containing any personal information is not permitted to leave the secure environment or to remain on any desk or workspace unattended overnight.

1.5) Staff authorised to process client personal information may only have one client's file at their workspace at any one time, said client file must be secured before a second or any subsequent files are worked on.

1.6) Archived files are stored behind locked doors and access control to these storage facilities are strictly controlled with only authorised, PSIRA registered security staff members permitted to enter.

1.7) All the user terminals on our computer network and our servers are protected by passwords and these are changed on a regular or regular/monthly basis depending on the user's access authority.

1.8) Our email infrastructure must comply with industry standard security and meet the General Data Protection Regulation (GDPR), which is standard in the European Union.

1.9) Vulnerability assessments are carried out on our digital infrastructure on a monthly basis to identify weaknesses in our systems and to ensure that we have adequate security in place.

1.10) We use an internationally recognised physical and digital Firewall to protect the data on our servers, and we continuously run ESET antivirus protection to ensure our systems are kept secure with the latest software.

1.11) Our staff must be trained to carry out their duties in compliance with POPI, and this training will be ongoing.

1.12) It is a term of the employment contract with every staff member that they must maintain full confidentiality in respect of all our client's affairs, including our client's personal information.

1.13) Employment contracts for staff whose duty it is to process a client's personal information includes an obligation on that staff member, to maintain the Company's security measures and to notify their manager/supervisor immediately, if there are reasonable grounds to believe that the personal information of a client has been accessed or acquired by any unauthorised person.

1.14) The processing of the personal information of our staff members takes place in accordance with the rules contained in the relevant labour legislation.

1.15) The digital work profiles and privileges of staff who have left our employ must be properly terminated and this includes removal of the staff member from our online PSIRA profile.

1.16) The personal information of clients and staff is destroyed timeously in a manner that de-identifies the person.

1.17) These security measures are verified on a regular basis to ensure effective implementation, and the safeguards must be continually updated in response to new risks or deficiencies.

1.18) All external agents/companies that process client information on behalf of Complex Patrols, are bound by contractual agreement to strictly adhere to the same stringent protection of client personal information as is required by law and according to Complex Patrols standards.

D. Security verification

1. Wherever possible and wherever mandatory, our authorised staff will **successfully** verify our client by means of requesting the following:

1.1**) for account related queries**: the client to confirm the unique Customer code and client cellphone number.

1.2**) for all security related verifications:** the client's secret password.

1.3**) for any corrections, alterations, or amendments to the security related information on record:** a complete a request form **(see form 2)** the client's secret password and a confirmation telephone call from an authorised staff member to the client confirming the changes requested.

1.4**) any hard copies of the client's personal information on record:** the client must present themselves in person at our business premises, with their SA identity document/valid passport.

1.5**) for changes to banking details:** presentation of a, SA Identity document/valid passport and the completed new debit order mandate to an authorised Complex Patrols staff member at our business premises or at the clients' premises on record.

1.6**) for all temporary changes to keyholders**: an email from the client stating such changes and a confirmation telephone call from an authorised staff member to the client confirming the changes requested.

E. Access to records from Complex Patrols

1. On request and after proper verification using any one method described in clause 2, any person is entitled to request that we confirm, free of charge, whether we hold any personal information about that person in our records.

2. If we do hold such personal information, on request **(see CP6 form C)** and upon identifying verification see (clause 2) and upon payment of a fee of R350-00 plus VAT *or an amount determined by the Information Regulator (*whichever is the lesser), we shall provide the person with the record, or a description of the personal information, including information about the identity of all third parties or categories of third parties who have or

have had access to the information. We shall do this within a reasonable period (not more than 30 days), in a reasonable manner and in an understandable form.

3. A client requesting such personal information must be advised of their right to request to have any errors in their personal information corrected, which request shall be made on the prescribed application form. **(See cp3 [form 2})**

4. In some circumstances, we will be required to refuse to disclose the record containing the personal information to the client. In other circumstances, we will have discretion as to whether to do so.

5. In all cases where the disclosure of a record will entail the disclosure of information that is supplementary to the personal information of the person requesting the record, the written consent of the Information Officer (or his deputy) will be required, and that person shall make their decision giving due consideration for the provisions contained Chapter 4 of Part 3 of the Promotion of Access to Information Act.

6. If a request for personal information is made and part of the requested information may, or must be refused, every other part thereof will still be disclosed.

7. For the exclusive purpose of any information requests or any other matter relating to the POPI act, our clients may use the following email address:

privacy-requests@complexpatrols.co.za

F. Correction of personal information of Complex Patrols Client

1. A client is entitled to require us to correct or delete personal information that we have, which is inaccurate, irrelevant, excessive, outdated, incomplete, misleading, or which has been obtained unlawfully.

2. A client is also entitled to expect that we will destroy or delete records of personal information about the client that we are no longer authorised to retain.

3. Any such request must be made on the prescribed form **(See cp3{form 2}).**

4. Upon receipt of such a lawful request, we must comply as soon as reasonably possible (within 30 days)

5. If a dispute arises regarding the client's rights to have information corrected and the request is in writing, we must attach this to the client's information, in a way that it will always be read with the information, as an indication that the correction of the information has been requested but has not been made.

6. We must notify the client who has made a request for their personal information to be corrected or deleted exactly what action we have taken.

G. Special personal information of Complex Patrols Client

1. Special rules apply to the collection and use of information relating to a person's religious or philosophical beliefs, their race or ethnic origin, their trade union membership, their political persuasion, their health or sex life, their biometric information, or their criminal behavior.
2. We shall not process any of this Special Personal Information without the client's consent.
3. It is unlikely that we will have to process special personal information in relation to our clients, but should it be necessary ONLY the Information Officer, or the deputy may process such.

Complex Patrols does not require, nor shall we ever collect or record anywhere, any personal information that identifies our clients by race, ethnic origin, sexual activity, philosophical or religious beliefs, political persuasion or trade union membership, health, or biometric information.

H. Processing personal information of a child (Minor) by Complex Patrols

1. We may only process the personal information of a child if we have the consent of the child's parent or legal guardian.

I. Information Officer

1. Our Information Officer is **Jacobus Van Rooyen (Jaco)**, our General Manager, nominated and authorised by Directors Barry Whittaker and Lourens Myburgh. **(See IR Authority)** Our Information Officer's responsibilities include:

   1.1 Ensuring compliance with POPI.

   1.2 Dealing with requests which we receive in terms of POPI.

   1.3 Working with the Information Regulator in relation to investigations.

   1.4 Facilitating ongoing POPI training and updating of staff.

   1.5 Manage any record of client's personal information in terms of ensuring the information is current and accurate.

.2. Our Information Officer must designate in writing as many Deputy Information Officers as are necessary to perform the tasks mentioned in paragraph 1 above. Such designation shall be done by the completion of the prescribed form and be made available upon request by any person.

3. Our Information Officer and our Deputy Information Officers have registered themselves with the Information Regulator prior to taking up their duties.

4. In carrying out their duties, our Information Officer must ensure that:

4.1 this Compliance Manual is implemented.

4.2 do regular or cause to be done a Personal Information Impact Assessment to ensure that adequate measures and standards exist to comply with the conditions for the lawful processing of personal information.

4.3 that this Compliance Manual is monitored, maintained and is available.

4.4 internal measures are developed with adequate systems to process requests for information or access to information.

4.5 that internal staff update sessions or refresher sessions are conducted regarding any new provisions of POPI, the Regulations, codes of conduct or information obtained from the Information Regulator.

4.6 that copies of this manual are provided to persons at their request, hard copies to be provided upon payment of a fee or R350.00 or (to be determined by the Information Regulator), whichever is the lesser.

5. Guidance notes on Information Officers have been published by the Information Regulator (on 1 April 2021) and our Information Officer and deputy Information Officers have familiarize themselves with the content of these notes.

6. Complex Patrols Directors remain ultimately responsible for POPI compliance and or any breach thereof and are guided by the Information Officer and deputies.

J. Authorisation request from the Information Regulator

1. Complex Patrols is a responsible security service provider and therefore strictly prohibits the disclosing of any form of client personal information by our staff, to any 3rd party while conducting our normal business or otherwise. If required to do so as a matter of law, we will need prior authorisation from the Information Regulator before processing any personal information such as,

1.1 In the unlikely event that we at Complex Patrols intend to utilise any unique identifiers of clients (account numbers, file numbers or other numbers or codes allocated to clients for the purposes of identifying them in our business) for any purpose other than the original intention, or to link the information with information held by others or,

1.2 if we are processing information on criminal behavior or unlawful or objectionable conduct or,

1.3 if we are processing information for the purposes of credit reporting or,

1.4 In the unlikely event that we at Complex Patrols, would need to transfer special personal information or the personal information of children to a third party in a foreign country, that does not provide adequate protection of that personal information.

2. The Information Regulator must be notified of our intention to process any personal information as set out in paragraph 10.1.1 above, prior to any processing taking place and we may not commence with such processing until the Information Regulator has decided in our favour. The Information Regulator has four weeks to decide but may decide that a more detailed investigation is required. In this event the decision must be made in a period as indicated by the Information Regulator, such a period must not exceed 13 weeks. If the Information Regulator does not decide within the stipulated time periods, Complex Patrols can assume that the decision is in our favour and commence processing the information.

K. Direct marketing of services

1. Complex Patrols **does not ordinarily direct market its service** and relies mainly on word of mouth, client recommendations, service accolades and visual presence in the area to promote our business, however, we may only carry out direct marketing (using any form of electronic communication) to clients if.

   1.1 the client was given an opportunity to object to receiving direct marketing material by electronic communication at the time that their personal information was collected.

   1.2 the client did not object then or at any time after receiving any such direct marketing communications from us.

2. We may only approach clients using their personal information, if we have obtained their personal information, in the context of providing services to them associated with business and even then, we may only market our core services.

3. We may only carry out direct marketing (using any form of electronic communication) to potential clients if we have received their consent to do so.

4. In the unlikely event, that we do approach a person to ask for their consent to receive direct marketing material from Complex Patrols, this approach may only occur once and if the person refuses consent, we may not approach this same person again for consent.

5. A request for consent to receive direct marketing from Complex Patrols must be made using the prescribed form for this request and consent. **(See cp5 {form 4})**

6. All direct marketing communications must disclose the identifying details of Complex Patrols, including the address and or other contact details to which the client may send a request that the communications cease.

L. Across borders information protection

1. Complex Patrols is not permitted to transfer a client's personal information to another person in a foreign country, unless:

    1.1 the client consents to this or requests it.

    1.2 the transfer of the personal information is required for the performance of the service contract between Complex Patrols and the client

    1.3 such a person is also subject to binding agreement which protects the personal information of our client in a manner that has the same or similar lawful effect as the POPI act, and such person is also subject to such or similar laws that prohibit the onward transfer of the personal information to another person in another country.

    1.4 the transfer is necessary for the conclusion or performance of a contract for the benefit of the client entered between Complex Patrols and the third party.

    1.5 the transfer of the personal information is for the benefit of the client and it is not reasonably possible to obtain their consent, and that if it were possible the client would likely give such consent.

M. Breach protocol

1. On first becoming aware that the personal information of a client has been accessed or acquired by an unauthorised person, our Information Officer must notify the Information Regulator and the relevant client. (if able to still identify the client) as soon as reasonably possible, taking the severity of the situation into consideration.
2. our Information Officer will notify the Information Regulator first, as it is possible that they, or another public body, might require the notification to the client be delayed.
3. To reasonably ensure client receipt of notification, such must be communicated in writing in one of the following methods:

    3.1) as directed by the Information Regulator.

    3.2) by mail to the client's last known physical or postal address.

    3.3) by email to the client's last known email address.

    3.4) by publication on our website or

    3.5) publication in the news media

4. This notification to the client must give sufficient information to enable the client to protect themselves against the potential consequences of the security breach, and must include:

    4.1) a description of the possible consequences of the breach.

4.2) details of the measures that we intend to take or have taken to address the breach.

4.3) the recommendation of what the client could do to mitigate the adverse effects of the breach.

4.4) the identity (if known) of the person who may have accessed or acquired the personal information.

N. Offences and penalties

1. It is of paramount importance that we comply strictly with the terms of this Compliance Manual and treat our client's personal information as private, privileged, with respect and protect this information as if it were our very own.

   1.1 Staff breaches of this Compliance Manual will also be viewed as a serious disciplinary offence.

2. The POPI act makes provision for penalties for the contravention of its terms, these are serious penalties such as.

   2.1 For minor offences a guilty party can receive a fine or be imprisoned for up to 12 months.

   2.2 For serious offences the period of imprisonment may be a maximum of 10 years.

   2.3 Administrative fines for the company can reach a maximum of R10 million.

Every effort will be made to protect and process personal information in a responsible and respectful manner, however, should it be discovered that this is not the case then the person may contact or lodge a complaint at

The information Regulator

33 Hoofd Street

Forum III, 3rd Floor Braampark

P.O Box 31533

Braamfontein, Johannesburg, 2017

Complaint's email: complaints.IR@justice.gov.za

General enquiries email: inforeg@justice.gov.za