THE PROTECTION OF PERSONAL INFORMATION OF SOCIAL GRANT BENEFICIARIES
This booklet on the protection of the personal information of social grant beneficiaries has been prepared for information and education purposes.

Our hope is that it will give you the information you need to raise awareness about the importance of protecting personal information, that of social grant beneficiaries in particular, and to assist you in protecting and helping those in your community.

While the Protection of Personal Information Act, 2013 (POPIA) was signed into law in 2013, it has not yet fully come into effect. Only certain limited provisions are currently in force, including:

- the definitions section;
- the provision establishing the new data protection authority (the Information Regulator); and
- the provision giving the Information Regulator power to make regulations under POPIA.

Final regulations were published under POPIA in December 2018 (although these are also not yet in force).

It is not yet clear when POPIA will come into force. Once POPIA is brought into effect, there will be an interim period of one year (which may be extended to three years) in which organisations are required to ensure compliance with POPIA.

Although POPIA is not yet fully in effect, organisations are generally taking steps to ensure compliance with POPIA now.

Fatima Laher  
Head of Pro Bono at Bowmans

Lynette Maart  
National Director at the Black Sash

Hoodah Abrahams-Fayker  
National Advocacy Manager at the Black Sash

This booklet has been prepared as if POPIA was in full force and effect.

When in doubt as to the steps that can be taken now, please contact the Black Sash Helpline or the office of the Information Regulator for further information. Contact details are included on page 56 of this booklet.
Contents

06  Glossary – important terms used in POPIA

10  A social grant beneficiary’s right to the protection of his or her personal information

14  Introduction to POPIA

20  The collection of personal information for social grants

30  The rights of applicants and beneficiaries in relation to their personal information

38  A practical toolkit

43  How the Black Sash can help – templates

56  Key contacts
Glossary – important terms used in POPIA

- **Biometrics** means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

- **Child** means a natural person under the age of 18 years who is not legally competent to take any action or decision about any matter concerning him- or herself without the assistance of a competent person.

- **Consent** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing or personal information.

- **CPS** are the Cash Paymaster Services.

- **Data subject** means the person to whom personal information relates (meaning, each individual person, you and me).

- **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.

- **DSD** is the Department of Social Development.

- **ECTA** is the Electronic Communications and Transactions Act.

- **NCA** is the National Credit Act.

- **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, 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; 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.

• **POPIA** is the Protection of Personal Information Act.

• **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.

• **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.

• **SAPO** is the South African Postal Office.

• **SASSA** is the South African Social Security Agency.
• **Special personal information** means personal information concerning:

  • the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a 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.
In South Africa, a person’s personal information is currently afforded general protections under the common law (e.g. previous decisions by the courts) and the South African Constitution. In terms of the common law and constitutional right to privacy (section 14), each person has a reasonable expectation of privacy, which may not be wrongfully or intentionally interfered with.

There are also a number of different laws that protect personal information (and therefore the privacy) of people, including any personal information provided when people apply for grants from the South African Social Security Agency (SASSA), as set out in further detail below. In this regard:

• POPIA and the regulations published under POPIA comprehensively protect the personal information of people (also called ‘data subjects’) by limiting when and how that information may be ‘processed’, including the collection, holding, use, sharing, or transferring of information, by the person in control of it (called a ‘responsible party’). In other words, POPIA sets out what personal information is, how it can be used, and what we can do to protect ourselves from people trying to exploit us by stealing or unlawfully using our information, particularly where we have not agreed to our information being used in this way.

• The Social Assistance Act specifically protects information about people who apply for social grants. This information is collected by SASSA and includes: an applicant’s name, age, nationality (or origin), physical address, financial information (including bank account details), medical information, identity number, and marital status. Under the Social Assistance Act, a person may only share the personal information of an applicant if doing
something in terms of the Social Assistance Act, when a law or a court tells that person to share the information, or when the applicant has agreed to his or her information being shared.

• The SASSA Act also protects information that is received when a person applies for a social grant application or a grant payment, benefit or assistance. Under the SASSA Act, a person may not disclose any information received as part of an application for a SASSA grant, payment, benefit or assistance, unless told to do so by a court or unless the person who made the application agrees in writing.

The SASSA Act authorises SASSA, with the agreement of the Minister of Social Development, to partner with another person to make sure that social grants are paid to beneficiaries. Any agreement with such a partner must include certain terms, including terms to make sure that the partner service provider does not share any personal information of applicants or beneficiaries of social grants without their consent or agreement. The agreement must also include fines if the terms of the agreement are not followed.

When considering the protection of social grant beneficiaries’ personal information, consideration must be given to the provisions of POPIA, the Social Assistance Act, the SASSA Act, as well as the common law and constitutional right to privacy. For the purposes of this booklet, the primary focus is on the provisions of POPIA, although consideration is also given to the all important laws as a whole.
Mamma Siski was living in Makwassie, a township outside of Wolmaranstad in the North West Province. Mamma Siski was 76 years and was getting the Older Persons grant. She sold roasted peanuts to try to earn some extra money so that she could survive.

Mamma Siski noticed that she had been getting much less pension money than she should.

Cash Paymaster Services (CPS) was given the contract to pay social grants in 2012 and Mamma Siski got her new ‘white’ SASSA card with the rest of grant beneficiaries in South Africa. Her problems started when she got the new SASSA card.

Money was being taken from her card before she could even collect her grant. A mini-statement showed a deduction of R190 from Moneyline and another deduction from a bank that cannot be identified.

Mamma Siski was not alone. Across the whole of South Africa grant beneficiaries were having the same problem. Money was going out of their SASSA accounts in the form of debit orders or EFTs for things like airtime, loans, electricity, multiple funeral cover insurance and even water.

What was going on?

CPS was linked to a bigger company called Net1 which has other companies (subsidiaries) that offer services like loans, funeral cover, airtime etc. It was alleged that CPS had given the personal private information of grant beneficiaries to Net1 and its subsidiaries who were using this information to market loans and funeral policies and make unlawful deductions for airtime and electricity that people had not agreed to.

To make matters worse, in order to sort out these problems, people were having to use even more money to travel to a SASSA office or to make phone calls to try to get their money back.

The Black Sash fought to fix this problem for many years, first by working with the Department of Social Development (DSD) and eventually by going to
Constitutional Court. The Constitutional Court then ruled that SASSA had a duty to protect the privacy of social grant beneficiaries’ personal data and that the data cannot be used for any purpose other than for payment of the grants. (Black Sash & Others v Minister of Social Development & Others CCT48/2017, Constitutional Court Order dated 17 March 2017, p.4.)

The story of Mamma Siski shows us why it is so important for us all to understand what private personal information is, how it can be used, and what we can do to protect ourselves from people trying to exploit us by stealing or unlawfully using our information, particularly where we have not agreed to our information being used in this way.

While the story of Mamma Siski relates to CPS as a private contractor, appropriate measures must be put in place in the current partnership between SASSA and the South African Post Office (SAPO), and any future partnership, so as to make sure that beneficiaries’ personal information is properly protected and to make sure that beneficiaries’ grants are not preyed upon by unscrupulous lenders who get access to beneficiaries’ personal information.

The Black Sash has always advocated for the protection of personal information to ensure that beneficiaries receive the full cash value of their grants without unauthorised and unlawful deductions.
Introduction to POPIA

POPIA is an important piece of legislation that provides for more comprehensive protection of personal information. It is important to understand what the Act says about personal information, how it is protected and what steps we can all take to protect our personal information.

POPIA places duties on organisations (or responsible parties) who are processing personal information and who decide how and why that personal information is processed. For example, POPIA places duties on SASSA for when and how beneficiaries’ personal information is processed.

POPIA does not change the existing requirements regarding the protection of personal information (under the common law and constitutional right to privacy), but it does improve the enforcement (compliance) mechanisms to ensure the protection of personal information. In other words, under POPIA it will be easier to take steps to protect our personal information.

What is personal information?

Personal information is any information that identifies a person who is alive. What identifies a person could be as simple as a name or number, or it could be something like another person’s views or opinions about that person.

Personal information can also include a person’s, race, gender, nationality (or origin), sexual orientation, age, physical or mental health, disability, language, birth, or whether a person is pregnant or married.

Personal information also includes a person’s ID number, contact details (such as a person’s physical address and telephone number), as well as a person’s medical, financial and employment information. It also includes ‘biometric information’, meaning a person’s fingerprints, photograph, and a recording of his or her voice.
‘De-identified’ information is information that cannot be used to identify any person. It is personal information that has been changed in some way by, for example:

- removing personal identifiers (such as a person’s name, address, date of birth or other identifying information); or
- removing or changing other information that may allow a person to be identified because of, for example, a rare characteristic of the person or a combination of characteristics that enable identification.

If any information has been ‘de-identified’, meaning that it does not relate to and identify a person, that information is not considered to be personal information under POPIA.

For example, the following paragraph:

‘Siski Dlamini was living in Makwasie, a township outside of Wolmaranstad in the North West Province. Siski Dlamini was 76 years and was getting the Older Persons grant. She sold roasted peanuts to try to earn some extra money so that she could survive.’

could be amended as follows:

‘Mamma S was living in a township outside Wolmaranstad in the North West Province. Mamma S was between the ages of 70 and 80 years and was getting the Older Persons grant. She sold food to try to earn some extra money to survive.’

Once a person has died, the information relating to that person is no longer considered to be personal information under POPIA (which only includes information relating to “living” natural persons).

What is special personal information, and how is it different from personal information?

Special personal information is information about a person’s religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information (e.g. a person’s fingerprints, photograph, and a recording of his or her voice) and criminal behaviour. This information is considered to be ‘sensitive’ personal information that should be treated with special care.

This means that special personal information is regulated separately under POPIA. The processing of special personal information, including the sharing of
that information with other people, is generally not allowed unless the person who that information is about has agreed (or ‘consented’) to the information being shared (or if there is another specific legal reason for sharing the information).

**What does ‘processing’ mean?**

‘Processing’ means any activity with personal information and includes: collecting, receiving, recording, organising, combining, storing, updating, retrieving, altering, consulting, using, sharing, merging, linking, restricting, erasing or destroying personal information.

**The conditions for lawful processing of personal information**

POPIA has a number of conditions for when personal information can be processed by or for an organisation (or responsible party), whether that party is SASSA, CPS, the South African Post Office (SAPO), etc. including the following:

- **Lawful processing:** Personal information can only be processed in terms of the law and in a reasonable way that does not interfere with the privacy of a person unnecessarily. For example, SASSA collects and processes certain personal information for the purposes of paying social grants to beneficiaries, in terms of the Social Assistance Act.

- **Reasonable processing:** Personal information may only be processed in an adequate (acceptable to meet the purpose for which the personal information is being processed), relevant (related to the purpose for which the personal information is being processed) and moderate (limited) way (meaning that an organisation does not hold more information than is needed for the purpose). For example, if SASSA requires that information on a person’s criminal behaviour is submitted with an application for a disability grant, it could be argued that it is irrelevant and excessive to obtain this information, and that this information should accordingly not be collected by SASSA.

- **Processing for a specific purpose:** Personal information must be collected for a specific, clearly defined and lawful purpose linked to a function or activity of the organisation. In other words, there must be a reason for the processing. For example, SASSA collects certain financial information from an applicant for the purpose of determining whether that applicant is eligible to receive a social grant.
• **Keeping personal information:** Records of personal information must not be kept any longer than is necessary for achieving the purpose for which it was processed. However, a record must be kept if (i) required under a law, (ii) the organisation needs the record for lawful purposes linked to its functions or activities, or (iii) it is a contractual requirement between the parties etc. For example, if a beneficiary is no longer eligible to receive a social grant, then SASSA should delete any information held about that beneficiary if it is no longer allowed or required to keep that information under the applicable law.

• **Quality of information:** The organisation must take steps to make sure that personal information that is processed is complete, correct, not misleading and kept up-to-date where necessary. For example, SASSA must take steps to ensure that a beneficiary’s name, contact details and banking details, where applicable, are up-to-date so as to enable the payment of the social grant to that person.

• **Security safeguards:** An organisation is required to make sure that it has put in place security measures to keep the personal information which it processes safe and confidential. This requires that the organisation takes appropriate, reasonable technical and organisational measures to prevent loss or damage to, or unauthorised destruction of, unlawful access to, or processing of personal information. For example, SASSA must ensure that it has taken appropriate steps and put in place appropriate measures to protect and keep safe any personal information that it holds about beneficiaries.

• **Openness:** When collecting personal information from a person, organisations must take steps to make sure that a person knows certain information like who is collecting the information and what they will be doing with that information. For example, when SASSA collects personal information from an applicant for a social grant, that applicant must understand exactly what information is being collected, why that information is being collected, and who will have access to that personal information.

• **Data subject participation:** Under POPIA, a person has the right to access and correct his or her personal information, the right to know the purpose for which his or her information is being processed and who will be receiving his or
her personal information, and the right to prevent the use of his or her personal information for direct marketing purposes. For example, if a beneficiary wants to know what personal information the SASSA holds about him or her, he or she can request access to that information held by SASSA and, if needs be, he or she can request that the information be corrected or deleted.

**The Information Regulator**

The Information Regulator is an independent body set up under section 39 of POPIA. The Information Regulator has the power to enforce and monitor compliance with POPIA. The Information Regulator is also responsible for making codes of conduct for different sectors and for making guidelines to assist organisations with the development and application of codes of conduct (although, to date, no codes of conduct have been published).

Any person may lay a complaint with the Information Regulator when his or her personal information has not been processed lawfully (see page 16 for an overview of the conditions for lawful processing) or when a responsible party has not complied with POPIA. After the complaint is made, the Information Regulator may investigate the complaint. The Information Regulator can also issue an enforcement notice to any organisation.

POPIA provides for various criminal offences (e.g. for a failure to comply with an enforcement notice or for making false statements). Penalties for criminal offences include a fine and/or up to 12 months’ or 10 years imprisonment, depending on the criminal offence. If a matter is not referred for criminal prosecution, an administrative fine (of a maximum of ZAR 10 million) may be imposed by the Information Regulator. The right to make a complaint with the Information Regulator is discussed in more detail on page 36.

On the request of a person, the Information Regulator may also institute a civil action claim for damages (money for any loss experienced) in a court against an organisation for not meeting any provision of POPIA, whether or not the organisation acted on purpose or not.

The Information Regulator’s contact details are:

E: inforeg@justice.gov.za
The collection of personal information for social grants

**Social grants: who collects the personal information?**

SASSA is responsible for managing social assistance, and SASSA (and its officials) are responsible for collecting and processing beneficiaries’ personal information, which is needed to assess applications for social grants, and paying social grants.

As permitted under the legislation, SASSA has made an agreement with SAPO to assist with the payment of social grants to beneficiaries on behalf of SASSA. Under this agreement, SASSA must share beneficiaries’ personal information with SAPO so that social grants are effectively distributed. The agreement between SASSA and SAPO is required to include protections which ensure that SAPO protects all personal information belonging to applicants for, and beneficiaries of, social grants.

SASSA previously had an agreement with CPS to distribute social grants to beneficiaries and SASSA similarly shared beneficiaries’ personal information with CPS for the purposes of distributing social grants.

**What personal information is collected by SASSA?**

The information that is collected from an applicant for a social grant includes information that identifies that applicant and the means (the financial position) of that applicant.

In general, when an applicant applies for a social grant, the following personal information is collected from him or her: name, age, nationality (or origin), physical address (and proof of residence), financial information (including bank account details, in certain instances, and income and assets), medical information, identity number (in the form of an identity document or birth certificate), marital status, and contact details. Fingerprints, a photograph, and sometimes a recording of a voice, are also collected.
How is the personal information collected, and who is this information collected from?

During the ‘application process’, all relevant personal information will be collected directly from the applicant.

An applicant completes a form in which he or she shares all the necessary information required for the purposes of working out if the applicant should receive a social grant and ensuring that, if applicable, a social grant is paid to him or her.

Once the information has been provided, a SASSA officer will confirm the information that has been given by an applicant to determine whether it is true and correct.

When, and under what conditions, can the personal information be processed?

In terms of POPIA, personal information must be processed lawfully and in a way that does not interfere with the privacy of a person unnecessarily. In this regard, personal information may only be processed if, given the purpose for which it is processed, the processing is adequate, relevant and not excessive (see page 16 for an overview of the conditions of lawful processing).

If you feel that more personal information is being collected about you than is necessary for the purposes of assessing your application for a social grant and paying your social grant (e.g. your political party or your religious views), please contact the Black Sash helpline for support and advice on 072 66 33 739 or help@blacksash.org.za.
In other words, only the minimum amount of personal information must be processed to fulfil a particular purpose. SASSA must hold that much information, but no more than is necessary.

POPIA provides that personal information may only be processed by SASSA (or a third party duly authorised by SASSA) if:

- **Reason 1**: the person (i.e. the subject of the personal information) agrees to the processing (this ‘consent’ must be a voluntary, specific and informed expression of will as discussed on page 25);
- **Reason 2**: the processing is necessary to give effect to a contract to which the person is a party;
- **Reason 3**: the processing is necessary to give effect to a legal obligation;
- **Reason 4**: the processing protects a (legitimate) interest of the person;
- **Reason 5**: the processing is necessary for the proper performance of a public law duty by a public body; or
- **Reason 6**: the processing is necessary for pursuing the legitimate interests of the organisation or of a third party who has been provided with the information.
SASSA will use applicants’ personal information to assess whether a person should receive social assistance (e.g. by checking that the applicant meets the financial requirements) and to make sure that a beneficiary is paid (e.g. by recording a beneficiary’s bank account details).

In this way, SASSA creates a national database of all applicants for, and beneficiaries of, social assistance. The personal information collected helps SASSA to keep a record of the grant beneficiaries. The sharing of personal information with SASSA assists SASSA in administering and making payment of social grants, especially when applicants have chosen to have their grants deposited into their private accounts.

**What should an applicant be told when his or her personal information is collected by SASSA?**

When collecting personal information from applicants, SASSA should take steps to make sure that the applicants know:

- the types of personal information being collected;
- the name and address of SASSA;
- the purpose for which the information is collected;
- whether the supply of the information by the applicant is voluntary or mandatory;
- the consequences of failing to provide the information;
- any particular law authorising or requiring the collection of the information; and
- any further information, such as the recipient or category of the recipients, the nature or category of the information and the existence of the right of access to information.

Steps should be taken to provide this information to the applicant before the applicant’s personal information is collected.

In terms of the Social Assistance Act and the SASSA Act, if the personal information is to be shared with any other person, SASSA must first obtain the applicant’s written agreement (except if the information is shared with a person who requires the information to perform a function in terms of these laws). This means that in general, an applicant must understand that his or her information will be shared, who it will be shared with, and why it will be shared, before giving his or her agreement.
Who keeps (or retains) the personal information, and how is it kept?

All the personal information that has been submitted by the applicant will be collected by the SASSA officer and will be stored in the SASSA database.

SASSA is required to make sure that it has put in place good security measures that protect the personal information. This requires SASSA to take appropriate, reasonable technical and organisational measures to prevent loss or damage to, unauthorised destruction of, unlawful access to, or processing of, personal information.

As discussed above, in terms of the Social Assistance Act, SASSA is also allowed to enter into agreements with any person for the purposes of ensuring effective payments to beneficiaries. For example, SASSA previously concluded a contract with CPS (and now with SAPO) for the purposes of ensuring effective payments to beneficiaries. As such, any person authorised in terms of an agreement concluded with SASSA to assist, may also keep the personal information of beneficiaries, and must ensure that this information is protected from unauthorised access.

What can the personal information be used for?

Personal information can only be used for the purpose for which it was processed. This means that SASSA (and any other third party assisting SASSA) is only allowed to use applicants’ and beneficiaries’ personal information for the purpose for which it was collected, which is to:

- evaluate applications for social assistance; and
- administer and pay social assistance to eligible beneficiaries.

How does a social grant beneficiary consent to payment of his or her grant into his or her private bank account, and what does ‘consent’ mean?

In terms of regulation 23 of the Regulations published under the Social Assistance Act, SASSA will pay a social grant:

- into a private bank account if the beneficiary has consented (agreed) to such payment in writing and in person to SASSA; or
- where consent cannot be provided, alternative arrangements have been made with SASSA.
This has resulted in SASSA insisting that a social grant beneficiary gives written consent by completing an Annexure C form (which has never been prescribed or formally published) for his or her grant to be paid into his or her personal bank account.

Previously, social grant beneficiaries provided their biometric information for this purpose, and the use of biometric information for the purposes of providing consent has been the subject of litigation with SASSA (see page 6 for a definition of ‘biometrics’). Going forward, we recommend that written consent should be provided by social grant beneficiaries unless SASSA specifically recognises the provision of biometric information as an ‘alternative arrangement’.

Under POPIA, ‘consent’ to the processing of personal information must be a voluntary, informed and specific expression of will. Any act (whether a written consent, or some positive act taken by a person) can be relied on for consent under POPIA provided that it is clear that this act provides a person’s agreement for the processing of personal information and that this consent is (i) voluntary, (ii) informed, and (iii) specific.

For the sake of completeness, under POPIA ‘consent’ must be:

- **Voluntary**: Consent should involve some type of positive agreement (or ‘opt-in’). Providing biometrics for a specific purpose or completing a duly completed Annexure C would likely be considered to be voluntary consent for the purposes of processing that information under POPIA.

- **Informed**: The consent form must be as clear and concise as possible so that a social grant beneficiary can easily understand what it is that
What can the personal information not be used for?

Personal information cannot be used for any purpose for which it was not originally collected or processed. In the context of social grants, this would mean that an applicant’s or beneficiary’s personal information cannot be shared with unauthorised third parties and cannot be used for any other purpose, other than to administer and make payment of social grants. For example, unless a beneficiary has given his or her consent or there is some other recognised legal ground:

- **SASSA, SAPO and any other authorised third parties are NOT allowed to use beneficiaries’ personal information for any purpose other than ensuring the payment of the social grant.**
- **SASSA, SAPO and any other authorised third parties are NOT allowed to share beneficiaries’ personal information with any other person, including any company in their groups.**

A beneficiary can withdraw consent at any time. Maintaining a clear record of any consent for the processing of personal information is very important for any responsible party (such as SASSA). A beneficiary should also keep a record of any withdrawal of consent.
• SASSA, SAPO, and any other authorised third parties are NOT allowed to use beneficiaries’ personal information for the purposes of marketing financial services, such as funeral services, airtime and small loans, to a beneficiary.

When can the personal information be shared with other people, and what can those people do with the personal information?

There is a general duty that personal information cannot be shared with a third party. The exceptions to this rule are where the person consents or agrees to his or her information being shared (see pages 6 and 25 for the meaning of ‘consent’), or where the sharing of the information is allowed by law and the person has been made aware of this before the processing of his or her information.

Further, in terms of the Social Assistance Act and the SASSA Act, if the personal information is to be shared with any other person, SASSA must obtain the applicant’s written agreement to the sharing of his or her information, if not shared for the purposes of the legislation. This means that an applicant must understand that his or her information will be shared, who it will be shared with, and why it will be shared, before giving his or her agreement.

However, in terms of the SASSA Act, SASSA is allowed, with the concurrence of the Minister, to enter into agreements with any person for the purposes of ensuring effective payments to beneficiaries. For example, SASSA previously concluded a contract with CPS (and now with SAPO) for the purposes of ensuring effective payments to beneficiaries.

While CPS was permitted to keep certain personal information of beneficiaries that was needed to make payment to them, it was required to ensure that this personal information was protected. The personal information kept by CPS could also only be used for the purpose for which it was originally collected, and could not be shared with other parties without the consent (or agreement) of the beneficiary. (It is not clear that CPS complied with these requirements, and it is alleged that CPS was responsible for the unauthorised sharing of beneficiaries’ personal information with other companies in the Net1 group.)
How long can the personal information be kept/retained, and what happens when it is no longer allowed to be kept?

In general, records of personal information must not be kept any longer than is necessary for achieving the purpose for which it was collected or processed unless:

- the law requires that it is kept;
- the organisation needs the record for lawful purposes related to its functions or activities;
- the keeping of the record is required by a contract between the parties; or
- the person has consented (agreed) to the keeping of the record (see pages 6 and 25 for the meaning of ‘consent’).

Records of personal information may also be kept for longer periods for historical, statistical or research purposes, provided that the organisation has put in place protections against the records being used for any other purposes.

An organisation must destroy or delete a record of personal information or de-identify (meaning that it cannot be used to identify any person) it as soon as possible after the organisation is no longer allowed to keep it. It must not be possible to reconstruct the record after it has been destroyed or deleted.

However, it should be noted that personal information must be kept for certain periods of time under specific legislation. For example:

- Under the National Credit Act 34 of 2005 (the NCA), read with the Regulations made in terms of the NCA, a credit provider is required to maintain records of all applications for credit, credit agreements and credit accounts for a period of three years after the end of the credit agreement. In other words, in assessing whether an entity is still permitted to hold personal information, it is necessary to consider whether any specific document retention periods are included in relevant laws and whether a data subject has consented (agreed) to his or her personal information being used for that purpose.

- As such, in the context of any alleged credit activities by the Net1 group of companies, such as the granting of a loan, it must be considered whether a social grant beneficiary gave consent (see pages 6 and 25 for the meaning of ‘consent’) for his or her personal information to also be processed for a loan. If so, that company would be allowed to keep the social grant beneficiary’s personal information for a period of three years after the end of any credit agreement.
What are the restrictions on the processing of personal information of children?

The personal information of a child cannot be processed unless the parents or guardian(s) of the child have consented (agreed) to the processing of his or her personal information (see pages 6 and 25 for the meaning of ‘consent’) or if the processing is necessary for the establishment, exercise or defence of a right or obligation in law.

Where it appears to be impossible to ask for consent, and sufficient protections have been provided to make sure that the processing does not negatively affect the privacy of the child, or the information concerning the child has been made publicly available, the processing of a child’s personal information is permitted.

The Information Regulator may also allow an organisation to process the personal information of children, if the organisation applies to do so, if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the child.
The rights of applicants and beneficiaries in relation to their personal information

The right to be notified (told) that personal information is being collected

When personal information is collected from an applicant or beneficiary, that applicant or beneficiary should be provided with certain information by SASSA, including:

• what personal information SASSA is collecting;
• the name and address of the person (i.e. SASSA) collecting the personal information;
• the purpose for which the personal information is collected (e.g. for the purposes of assessing eligibility for a social grant and ensuring effective payment of that social grant in due course);
• whether the applicant must provide the information, or whether it is voluntary to do so;
• if the personal information is going to be transferred outside of South Africa, information on the country involved and what will be done with the data;
• the consequences of failure to provide the information (e.g. that eligibility for a social grant cannot be assessed, or that a social grant cannot be effectively distributed to a beneficiary);
• any particular law authorising or requiring the collection of the information; and
• any further information, such as the recipient or category of the recipients (e.g. such as a third party service provider like CPS or SAPO), the nature or category of the information, the existence of the right of access to information, and the details of the Information Regulator.
This is sometimes referred to as ‘privacy information’. Steps should be taken to provide this information to the applicant before the applicant’s personal information is collected. This information is usually included in the terms and conditions or contract signed by a person; there is no requirement for written confirmation.

If a beneficiary has concerns about how SASSA, SAPO, or any other related third party has handled his or her personal information, he or she can use the form published in the Regulations (template letter included on page 43) to raise these concerns with the relevant regulatory authorities.

**The right to be notified (told) that personal information has been accessed or acquired by an unauthorised person**

If an applicant’s or beneficiary’s personal information has been accessed or acquired by a person who is not allowed to access this information (i.e. if there is a data breach), the responsible party (i.e. SASSA) must notify the Information Regulator and, if the identity of a person can be established, the applicant or beneficiary him or herself.

This notification must be made as soon as possible after the discovery of the data breach or ‘security compromise’ (leaking of information). It must be in writing and must be sent to the applicant or beneficiary by post, by email, by being placed in a noticeable position on the organisation’s website, by being published in the news media, or as set out by the Information Regulator.

This notification must contain enough information to allow the applicants or beneficiaries to take steps to protect their personal information, and must include:

- a description of the possible consequences of the data breach;
- a description of the measures that the organisation intends to take or has taken to address the data breach;
- a recommendation of the measures to be taken by the applicant or beneficiary to mitigate the possible negative effects of the data breach; and
- if known to the organisation, the identity of the unauthorised person who may have accessed or acquired the personal information.

The Information Regulator may also tell an organisation to make public the fact of any data breach if the Information Regulator believes that such publicity would protect a person who has been affected by the data breach.
The right to establish whether an organisation holds personal information about the person, and to request access to that personal information

Any person, having provided adequate proof of identity, has the right to find out if an organisation is using or storing his or her personal information. This is often referred to as the ‘right of access’. A person can exercise this right by, in writing:

- asking the organisation to confirm, at no fee, whether or not the organisation holds personal information about him or her; and
- asking the organisation for the record or a description of the personal information about him or her held by the organisation, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information.

A record or description of the personal information held by an organisation about a person can be requested within a reasonable time, at the fee that has been set, in a reasonable manner or format, and in a form that is generally understandable. An organisation must give the person a written estimate of the fee before providing the record, and may ask the person to pay a deposit for all or part of the fee.

If personal information is communicated to a person who has requested access, that person must also be advised of his or her right to correct the information (see page 36). If an organisation needs more information to help it find a person’s information or identify a person, it will ask for additional information.

An organisation may refuse someone’s access request if the information requested includes information about another person, unless that person has consented to or agreed (see pages 6 and 25 for the meaning of ‘consent’) to the disclosure or it is reasonable to provide this information without the other person’s consent.

The right to request the correction, destruction or deletion of personal information

A person can challenge the accuracy or correctness of the personal information held about him or her and ask for it to be corrected or deleted (or destroyed).
In this regard, a person may, in the manner set out by the Information Regulator, ask an organisation to:

- correct (i.e. by adding more details) or delete personal information about the person in its possession or under its control that is inaccurate, irrelevant, excessive, outdated, incomplete, misleading or obtained unlawfully; or
- destroy or delete a record of personal information about the person that the organisation is no longer allowed to keep.

In this regard, a person’s request for correction or deletion of personal information must be in writing on a form that corresponds substantially with the relevant form as published in the Regulations (Form 2 – see page 47).

This form requires the submission of the following information:

- the name, identity number and contact details of the person;
- the details of the organisation; and
- detailed reasons for the request for correction or deletion of the personal information.

This form must then be signed and dated by the person. Affidavits or documentary evidence in support of the request can also be attached. An organisation is required to assist, to the best of its ability, any person who requires assistance with the completion of Form 2 (see page 47).

When an organisation is asked to correct data, it should take reasonable steps, as soon as possible, to investigate whether the data is accurate, and should be able to demonstrate it has done so. To do this, the organisation should consider a person’s arguments and any evidence provided.

When an organisation is asked to destroy or delete a record of personal information, it must do so if the organisation is no longer allowed to keep or retain that personal information. The organisation should then contact the person and either:

- confirm it has corrected, destroyed, deleted or added to the information; or
- inform the person that it will not correct the information, and explain, with credible evidence, why it believes the information is accurate.
Where the organisation has a reason not to agree with the person’s request to correct the information (see page 36), the person can ask for the organisation to attach a notice to the information confirming that a person has requested that the information be corrected, but that this request was not granted.

The right to deletion is not absolute and the organisation can refuse to delete the information in certain circumstances (e.g. when the organisation is legally obliged to keep the information, or keeping the information is necessary for the purposes of legal claims).

The right only applies in the following circumstances:

- the organisation no longer needs the information;
- the person initially consented (agreed) to the use of the information but has now withdrawn his or her consent;
- the person has objected to the use of his or her information;
- the organisation has collected or used the information unlawfully; or
- the organisation has a legal obligation to delete the information.

If the organisation has disclosed the personal information to others, it must contact them and tell them the personal information has been corrected or deleted.

The right to object to the processing of personal information

A person has the right to object to the processing (use) of his or her personal information, at any time, in certain circumstances including:

- If an organisation is processing personal information on the grounds, for example, that the processing is necessary for pursuing the legitimate interests of the organisation or a third party to whom the information is supplied. If an organisation agrees to the objection, it must stop using the personal information for that purpose unless it can give strong and legitimate reasons to continue using the information despite the person’s objections.

- For purposes of direct marketing, other than direct marketing by unwanted electronic communications (which is regulated separately under POPIA). In other words, a person has an absolute right to object to an organisation using his or her personal information for direct marketing (i.e. trying to sell things to the person). This means that the organisation must stop using the personal information if the person objects.
A person’s objection must be in writing on a form that corresponds substantially with the relevant form as published in the Regulations (Form 1 – see page 45). This form requires the submission of the following information:

- the name and contact details of the person;
- the details of the organisation; and
- detailed reasons for the objection.

This form must then be signed and dated by the person. An organisation is required to assist, to the best of his or her ability, any person who requires assistance with the completion of Form 1.

**The right not to have personal information processed for direct marketing by electronic communications**

At the moment, under the Electronic Communications and Transactions Act (ECTA), where an organisation sends unwanted commercial communications (like an sms or email) where no previous agreement to the communications has been given, consumers must be allowed to opt-out (say ‘no’).

This ability to opt-out must be included in the sms or email and the organisation must, on request, provide the consumer with information about where it got a consumer’s contact details. Failing to comply with ECTA is an offence.

POPIA has introduced new requirements for marketing directly to a person using electronic communications (email, sms, automated voice messages, but excluding telephone calls). In terms of POPIA, direct marketers are only able to use a person’s personal information (e.g. his or her names, contact details and other personal information) for direct marketing after getting the specific approval of a person. In other words, a person will have to opt-in (say ‘yes’) in order for direct marketing to be sent to him or her lawfully.

An organisation may ask a person (who has not previously said no) only once for his or her agreement to process his or her personal information for direct marketing. Form 4 under the Regulations sets out what information is required from a person for consent (see also pages 6 and 25 for the meaning of ‘consent’).
A person must still be allowed to object to the use of his or her personal details (i.e. to opt-out) both when the personal information is collected and every time a communication is sent to the person for the purposes of direct marketing. The opportunity to opt-out must be given to the person for free, and must be easy to do.

The right to send a complaint to the Information Regulator

Any person may send a complaint to the Information Regulator in Form 5 of the Regulations (see page 49) claiming interference with the protection of his or her personal information. A complaint must be in writing, and the Information Regulator must help a person to put a complaint in writing.

The Information Regulator may also start an investigation into the interference with the personal information of a person.

On receiving a complaint, the Information Regulator may:

- conduct a pre-investigation;
- act, at any time during the investigation, as conciliator;
- decide to take no action on the complaint or require no further action to be taken on the complaint;
- conduct a full investigation of the complaint;
- refer the complaint to the Enforcement Committee (a group of people within the Information Regulator responsible for making sure that POPIA is complied with); or
- take any further action, as required.

The Information Regulator must, as soon as possible, tell the complainant and the organisation what it has decided to do.

Usually, an enforcement notice will be issued by the Information Regulator if POPIA has not been complied with. POPIA also sets out various criminal offences (e.g. for a failure to comply with an enforcement notice or for making false statements). Penalties for criminal offences include a fine and/ or up to 12 months' imprisonment. The alternative to criminal prosecution is an administrative fine (of a maximum of ZAR 10 million).

The right to start civil proceedings regarding the alleged interference with the protection of personal information

A person or the Information Regulator, on the request of a person, may bring a civil action for damages (money for any loss experienced) in a court against an organisation for not complying with POPIA, whether or not there is intent or negligence on the part of the organisation.
A court may award an amount that is just and equitable (fair) including:

- payment of damages (money) as compensation for loss suffered by a person as a result of breach of the provisions of POPIA;
- aggravated damages (further damages in special cases), in a sum determined by the court;
- interest; and
- legal costs, as determined by the court.
A practical toolkit

A practical example: What are a person’s rights in relation to the personal information held by CPS/Grindrod?

In 2012 and 2013, following the contract concluded by SASSA with CPS, bank accounts were opened with Grindrod for over 10 million social grant beneficiaries.

Forty thousand beneficiaries chose to use bank accounts other than those held with Grindrod Bank. Approximately 1.1 million beneficiaries who were Grindrod account holders, chose to open EasyPay Everywhere (EPE) accounts with Grindrod from June 2015. Millions of other beneficiaries of social grants received their grants manually at cash pay points.

Evidence has been found that companies with links to Net1 had offered financial products including microloans to grant beneficiaries. It appeared that confidential information related to the Grindrod accounts was leaked and that there had been a breach of the integrity of the data within the payment system.

Government was concerned as it considered these practices to be in contravention of the Social Assistance Act, the SASSA Act and the applicable regulations. These allegations of a breach of data integrity were denied by Net1 and others.

Irrespective of whether or not these allegations are correct, it seems clear that grant beneficiaries’ personal information is currently being held and used by entities for purposes other than those consented (agreed) to by beneficiaries. Even to the extent that beneficiaries consented (agreed) to the use of their information in this manner, beneficiaries would have the right to withdraw their consent at any stage.

What can you advise a beneficiary to do:

- **Option 1:** A beneficiary can make a written request directly to CPS, Net1 and/or any Net1 company asking whether they hold personal information about him or her. Please see the template letter on page 43 for this purpose.

- **Option 2:** A beneficiary can make a written request for access directly to CPS, Net1 and/or any Net1 company, stating clearly what is wanted (e.g. the record or description of personal information about the beneficiary.
held by the relevant entity/ies). Please see the template letter on page 43 for this purpose.

• **Option 3:** A beneficiary can make a written request to CPS, Net1 and/or any Net1 company, through the submission of a completed Form 2, for the relevant entity/ies to immediately delete (destroy) any of his or her personal information that these entities hold, on the grounds that they are not authorised to keep or process his or her personal information. For the avoidance of doubt, it may also be advisable for a beneficiary to expressly withdraw any consent that he or she may have given to these entities, at any stage, for the processing of his or her personal information.

• **Option 4:** A beneficiary can expressly object to the processing of his or her personal information by CPS, Net1 and/or any Net1 company, by submitting a completed Form 1 directly to the relevant entity/ies.

• **Option 5:** A beneficiary can make a written complaint to the Information Regulator about the alleged interference with his or her personal information by completing and submitting Form 5.

Please note that while this practical example relates to the personal information held by CPS/Grindrod, the steps set out above would be applicable to ANY ORGANISATION holding personal information about the beneficiary.

Be careful of what is agreed to: some advice for beneficiaries

A beneficiary must be careful what he or she agrees to in any document. If a beneficiary does not understand what the document says, he or she must not sign the document.

If asked, a beneficiary should not agree to his or her personal information being used for any reason other than the payment of his or her social grant.

If a beneficiary receives a call from any person trying to sell something, like financial services, where the beneficiary did not ask for the call, the beneficiary should tell the caller to stop contacting him or her immediately and to remove his or her personal information from their records. This is called ‘opting out’. If a beneficiary has asked them to stop contacting him or her, that person is not allowed to contact the beneficiary any more.
**How to find out whether a person holds personal information about a beneficiary**

To exercise the right of access, the following practical steps should be followed:

- **Step 1:** Identify where to send a request and think about what personal information the beneficiary wants to access.

- **Step 2a:** Make a written request directly to the organisation asking whether it holds personal information about the beneficiary. Make sure that you attach adequate proof of the beneficiary’s identity (e.g. identity document, etc.). Ask for assistance where required. No fee must be paid. Any verbal request must be followed up in writing as this will provide clear proof of actions taken if a challenge of the organisation’s initial response is required.

- **Step 2b:** Make a written request directly to the relevant organisation and state clearly what is wanted (e.g. the record or description of personal information about the beneficiary held by the organisation). Make sure that you attach adequate proof of the beneficiary’s identity (e.g. identity document, etc.). Ask for assistance where required. The following information should be included when making this request:
  - the beneficiary’s name and contact details;
  - any information used by the organisation to identify the beneficiary or distinguish the beneficiary from other people with the same name (e.g. account number); and
  - any details or relevant dates that will help the organisation identify what is being requested.

The organisation must give a written estimate of the fee before providing the record and may ask for a deposit.

- **Step 3:** Keep a copy of any request and keep any proof of delivery.

*An example of such a written request is included on page 43.*
How to object to the processing of a beneficiary’s personal information

To object to the processing of a beneficiary’s personal information, the following practical steps should be followed:

• **Step 1:** Before objecting, the beneficiary may need to ask the organisation why it is processing his or her information. This is because a beneficiary can only object to processing where the organisation is processing it on certain grounds (e.g. legitimate interests) or for the purposes of direct marketing (other than direct marketing by unsolicited (unwanted) communications).

• **Step 2:** Identify where to send an objection and think about the basis on which the beneficiary wants to object to the processing of his or her personal information.

• **Step 3:** Make a written request in the prescribed form (Form 1 – see page 45) directly to the organisation. The following information must be included in the form:
  - the beneficiary’s name and contact details;
  - the details of the organisation; and
  - detailed reasons for the objection.

Ask an organisation for assistance to complete the form, if required. Also ask the Information Regulator or Black Sash for assistance, if needed, to properly set out:

- the reasons for the objection;
- the reasons must relate to the beneficiary’s particular situation; and
- why the beneficiary believes the organisation should stop using his or her information in this way.

Make sure that the beneficiary signs and dates the form.

• **Step 4:** Keep a copy of any objection and keep any proof of delivery.

• **Step 5:** If the beneficiary is unhappy with how the organisation has handled the request, the beneficiary should first complain to the organisation and, if he or she is still dissatisfied, the beneficiary can make a complaint to the Information Regulator.
How to opt out of direct marketing by means of unwanted electronic communications (emails and SMSs)

If a beneficiary receives an email, SMS or WhatsApp trying to sell him or her something, like financial services, where he or she did not ask for the contact, the beneficiary can tell the contactor to stop contacting him or her immediately and to remove his or her personal information from the contactor’s records. This is called ‘opting out’.

If the beneficiary has asked the contactor to stop contacting him or her, that person or organisation is not allowed to contact him or her anymore. A beneficiary can also submit a complaint to the Information Regulator if he or she has been contacted for direct marketing purposes, where he or she did not agree to being contacted in this way.

How to submit a complaint to the Information Regulator

To submit a complaint to the Information Regulator, the following practical steps should be followed:

• **Step 1:** Identify where to send a complaint and think about the basis on which the beneficiary wants to submit a complaint.

• **Step 2:** Complete the prescribed form (Form 5 - see page 49), setting out the alleged interference with the beneficiary’s personal information, and submit it directly to the Information Regulator. The following information must be included in the form:
  - the beneficiaries name and contact details;
  - the details of the organisation; and
  - detailed reasons for the complaint.

Affidavits or other documentary evidence can also be attached to the form. Ask the Information Regulator or Black Sash for assistance, if required, to enable you to put the beneficiary’s complaint in writing. Make sure that the beneficiary signs and dates the form.

• **Step 3:** Keep a copy of any complaint submitted to the Information Regulator and keep any proof of delivery.
How the Black Sash can help – templates

Template letter: Request for access to personal information held by company/organisation

[Data subject’s full address]
[Phone number]
[Date]
[Name and address of the organisation]

Dear Sir or Madam

Request for access to personal information held by [organisation]

My name is [•] (South African identity number [•]). [Insert any other details to help identify the data subject and the data you are requesting. For example: I am a recipient of a [grant] from the South African Social Security Agency (SASSA).]

In terms of section 23 of the Protection of Personal Information Act 4 of 2013, I am entitled to receive confirmation, free of charge, of whether you hold personal information about me and to receive a record of the personal information about me that is held by you. Accordingly, please confirm whether you hold personal information about me and, if you do, please supply this information to me.

OR - when you know what information you want to request:

In terms of section 23 of the Protection of Personal Information Act 4 of 2013, I am entitled to receive confirmation, free of charge, of whether you hold personal information about me and to receive a record of the personal information about me that is held by you. Accordingly, please supply data about me relating to:

[give specific details of the data you want, for example:

- my personnel file
- account details of bank accounts held by me
- biometric information about me
- emails between ‘person A’ and ‘person B’ (from [date] to [date])
- my medical records (between [year] and [year]) held by ‘Dr [•]’ at ‘hospital [•]"
• footage from CCTV camera situated at (‘location E’) on 23 May 2017 between 11am and 5pm
• copies of bank statements (between 2013 and 2017) held in account number[•].]

If you need any more information from me, or a fee, please let me know as soon as possible. Please note that data protection law requires you to respond to a request for access to information within a reasonable time of the request being made.

If you do not normally deal with these requests, please pass this letter to your Information Officer, or relevant staff member. If you need advice on dealing with this request, the Information Regulator’s office can assist you. Its website is www.justice.gov.za/inforeg/ or it can be contacted on 012 406 4818.

Yours faithfully
[Signature]

Copies of the applicable forms, which can be accessed on the Black Sash website, are included on the following pages.
FORM 1
OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF
SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013
(Act No. 4 of 2013)
REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 2]

Note:

1. Affidavits or other documentary evidence as applicable in support of the objection may be attached.
2. If the space provided for in this form is inadequate, submit information as an Annexure to this form and sign each page.
3. Complete as is applicable.

<table>
<thead>
<tr>
<th>A</th>
<th>DETAILS OF DATA SUBJECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name(s) and surname/registered name of data subject:</td>
<td></td>
</tr>
<tr>
<td>Unique Identifier/Identity Number:</td>
<td></td>
</tr>
<tr>
<td>Residential, postal or business address:</td>
<td>Code: ( )</td>
</tr>
<tr>
<td>Contact number(s):</td>
<td></td>
</tr>
<tr>
<td>Fax number/ E-mail address:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B</th>
<th>DETAILS OF RESPONSIBLE PARTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name(s) and surname/registered name of data subject:</td>
<td></td>
</tr>
<tr>
<td>Unique Identifier/Identity Number:</td>
<td></td>
</tr>
<tr>
<td>Residential, postal or business address:</td>
<td>Code: ( )</td>
</tr>
<tr>
<td>Contact number(s):</td>
<td></td>
</tr>
<tr>
<td>Fax number/ E-mail address:</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C</th>
<th>REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f) (Please provide detailed reasons for the objection)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Signed at........................................................................................................this...........day of.................................20............

...................................................................................................................

Signature of data subject/designated person
FORM 2
REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.4 OF 2013)
REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 3]

Note:

1. Affidavits or other documentary evidence as applicable in support of the request may be attached.
2. If the space provided for in this form is inadequate, submit information as an Annexure to this form and sign each page.
3. Complete as applicable.

Mark the appropriate box with an ‘x’.

Request for:

- Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.
- Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

<table>
<thead>
<tr>
<th>A</th>
<th>DETAILS OF DATA SUBJECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name(s) and surname/registered name of data subject:</td>
<td></td>
</tr>
<tr>
<td>Unique Identifier/Identity Number:</td>
<td></td>
</tr>
<tr>
<td>Residential, postal or business address:</td>
<td>Code: (                 )</td>
</tr>
<tr>
<td>Contact number(s):</td>
<td></td>
</tr>
</tbody>
</table>
### B DETAILS OF RESPONSIBLE PARTY

<table>
<thead>
<tr>
<th>Name(s) and surname/Registered name of responsible party:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Residential, postal or business address:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Code: ( )</td>
</tr>
<tr>
<td>Contact number(s):</td>
<td></td>
</tr>
<tr>
<td>Fax number/ E-mail address:</td>
<td></td>
</tr>
</tbody>
</table>

### C INFORMATION TO BE CORRECTED/DELETED/DESTRUCTED/DESTROYED

### D REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN.

(Please provide detailed reasons for the request)

---

Signed at....................................................................................this........day of.........................20.............

Signature of data subject/designated person
FORM 5
COMPLAINT REGARDING INTERFERENCE WITH THE PROTECTION OF PERSONAL INFORMATION/COMPLAINT REGARDING DETERMINATION OF AN ADJUDICATOR IN TERMS OF SECTION 74 OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [Regulation 7]

Note:

1. Affidavits or other documentary evidence as applicable in support of the request may be attached.
2. If the space provided for in this form is inadequate, submit information as an Annexure to this form and sign each page.
3. Complete as is applicable.

Mark the appropriate box with an ‘x’.

Request for:

- Alleged interference with the protection of personal information.
- Determination of an adjudicator.

<table>
<thead>
<tr>
<th>PART I</th>
<th>ALLEGED INTERFERENCE WITH THE PROTECTION OF THE PERSONAL INFORMATION IN TERMS OF SECTION 74 (1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (Act No. 4 of 2013)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>PARTICULARS OF COMPLAINANT</td>
</tr>
<tr>
<td>Name(s) and surname/registered name of data subject:</td>
<td></td>
</tr>
<tr>
<td>Unique Identifier/Identity Number:</td>
<td></td>
</tr>
<tr>
<td>Residential, postal or business address:</td>
<td></td>
</tr>
<tr>
<td>Code: ( )</td>
<td></td>
</tr>
<tr>
<td>Contact number(s):</td>
<td></td>
</tr>
<tr>
<td>Fax number/ E-mail address:</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>---</td>
</tr>
</tbody>
</table>

**B**  
PARTICULARS OF RESPONSIBLE PARTY INTERFERING WITH PERSONAL INFORMATION

<table>
<thead>
<tr>
<th>Name(s) and surname/ registered name of responsible party:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Residential, postal or business address:</td>
<td></td>
</tr>
<tr>
<td>Contact number(s):</td>
<td></td>
</tr>
<tr>
<td>Fax number/ E-mail address:</td>
<td></td>
</tr>
</tbody>
</table>

**C**  
REASONS FOR COMPLAINT (Please provide detailed reasons for the complaint)

**PART II**  
COMPLAINT REGARDING DETERMINATION OF ADJUDICATOR IN TERMS OF SECTION 74(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

**A**  
PARTICULARS OF COMPLAINANT

<table>
<thead>
<tr>
<th>Name(s) and surname/ registered name of data subject:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique Identifier/ Identity Number:</td>
<td></td>
</tr>
<tr>
<td>Residential, postal or business address:</td>
<td></td>
</tr>
</tbody>
</table>

Code: (   )
<table>
<thead>
<tr>
<th>Contact number(s):</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fax number/ E-mail address:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>B</strong> PARTICULARS OF ADJUDICATOR AND RESPONSIBLE PARTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name(s) and surname/registered name of responsible party:</td>
</tr>
<tr>
<td>Residential, postal or business address:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contact number(s):</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fax number/ E-mail address:</td>
<td></td>
</tr>
</tbody>
</table>

| **C** REASONS FOR COMPLAINT *(Please provide detailed reasons for the grievance)* |
|------------------------------------------|----------------------------------|
|                                          |                                  |
|                                          |                                  |
|                                          |                                  |

Signed at...................................................................................................................................this...........day of..............................20............

..........................................................................................................
Signature of data subject/designated person
Guidance notes to assist with completing forms

This guidance note has been prepared based on the forms as set out in the Regulations relating to the Protection of Personal Information, 2018.

FORM 1 – Objection to the processing of personal information in terms of section 11(3) of the POPIA.

# Task List:  
Completed:

1. Do you know the full name and surname of the data subject (i.e. your client)?
2. Do you know the identity number of the data subject?
3. Do you know the residential/ postal/ business address of the data subject?
4. Do you know the contact number(s) of the data subject?
5. Do you know the fax number / email address of the data subject?
6. Has the data subject provided you with a reason for objecting to the processing of his/ her personal information?

These reasons may include, for example:

• where the responsible party is processing the information for itself or for a third party and the data subject no longer wants his/ her information to be processed; or
• where the data subject no longer wants to be subjected to direct marketing (i.e. where the responsible party is trying to sell things to the data subject), other than direct marketing by unwanted electronic communications (which is regulated separately under POPIA)
7. Have you attached any relevant documentary evidence, or any affidavits the data subject may have deposed to with regard to his or her objection and reasons therefore? Please ensure that each page is signed.

8. Has the data subject signed and dated the bottom of the last page of the form?

9. Have you provided the data subject with a copy of the completed form?

**If the responsible party (i.e. the entity using/ in possession of the client’s information) is a natural person, complete this section:**

10. Do you know the name and surname of the responsible party?

11. Do you know the residential, postal or business address of the responsible party?

12. Do you know the contact number(s) of the responsible party?

13. Do you know the fax number/ email address of the responsible party?

**If the responsible party (the entity using/ in possession of the client’s information) is a public or private body or company, complete this section:**

14. Do you know the registered name of the responsible party?

15. Do you know the business address of the responsible party?

16. Do you know the contact number(s) of the responsible party?

17. Do you know the fax number/ email address of the responsible party?
FORM 2 – Request for correction or deletion of personal information or destruction or deletion of record of personal information in terms of section 24(1) of POPIA

<table>
<thead>
<tr>
<th>#</th>
<th>Task List:</th>
<th>Completed:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Has the data subject (your client) indicated whether he/ she needs the responsible party (the entity using/ in possession of the client’s information) to:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• correct or delete his/ her personal information which the responsible party has in its possession/ control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• destroy or delete his/ her personal information which the responsible party has in its possession/ control which it is no longer allowed to retain</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Do you know the full name and surname of the data subject?</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Do you know the identity number of the data subject?</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Do you know the residential/ postal/ business address of the data subject?</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Do you know the contact number(s) of the data subject?</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Do you know the fax number/ email address of the data subject?</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Do you know the name (and surname if a natural person) of the responsible party?</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>Do you know the residential/ postal/ business address of the responsible party?</td>
<td></td>
</tr>
</tbody>
</table>
9. Do you know the contact number(s) of the responsible party? 

10. Do you know the fax number/ email address of the responsible party? 

11. Has the data subject provided you with a reason for wanting the information to either be corrected/ deleted or destroyed? 

   If the data subject wants to correct incorrect information, in his/ her reason he/ she must set out what information he/ she believes to be wrong or incomplete and explain what the correct information is. Documentary evidence of the inaccuracies can be provided. 

12. Have you explained to the data subject that the right to deletion is not absolute and the responsible party can refuse to delete the information in certain circumstances (e.g. where it is legally obliged to keep the information, or where the information is necessary for the purposes of legal claims)? 

13. Have you attached any relevant documentary evidence, or any affidavits the data subject may have deposed to with regard to his/ her objection and reasons therefore? Please ensure that each page is signed. 

14. Has the data subject signed and dated the bottom of the last page of the form? 

15. Have you provided the data subject with a copy of the completed form?
Key Contacts

BLACK SASH
Contact the Black Sash helpline for support and advice on 072 66 33 739 or info@blacksash.org.za.

SASSA
Lodge a complaint with SASSA:
Contact the Call Centre: 0800 601011
or phone their landline: 012 400 2322
or report the complaint to a local SASSA office.

INFORMATION REGULATOR
Lodge a written complaint with the Information Regulator in the prescribed form (see Form 5) by email, post, facsimile, or personal delivery. The Information Regulator’s contact details are:
33 Hoofd Street
Forum III, 3rd Floor Braampark
Braamfontein, Johannesburg
Tel: 012 406 4818
Fax: 086 500 3351
inforeg@justice.gov.za