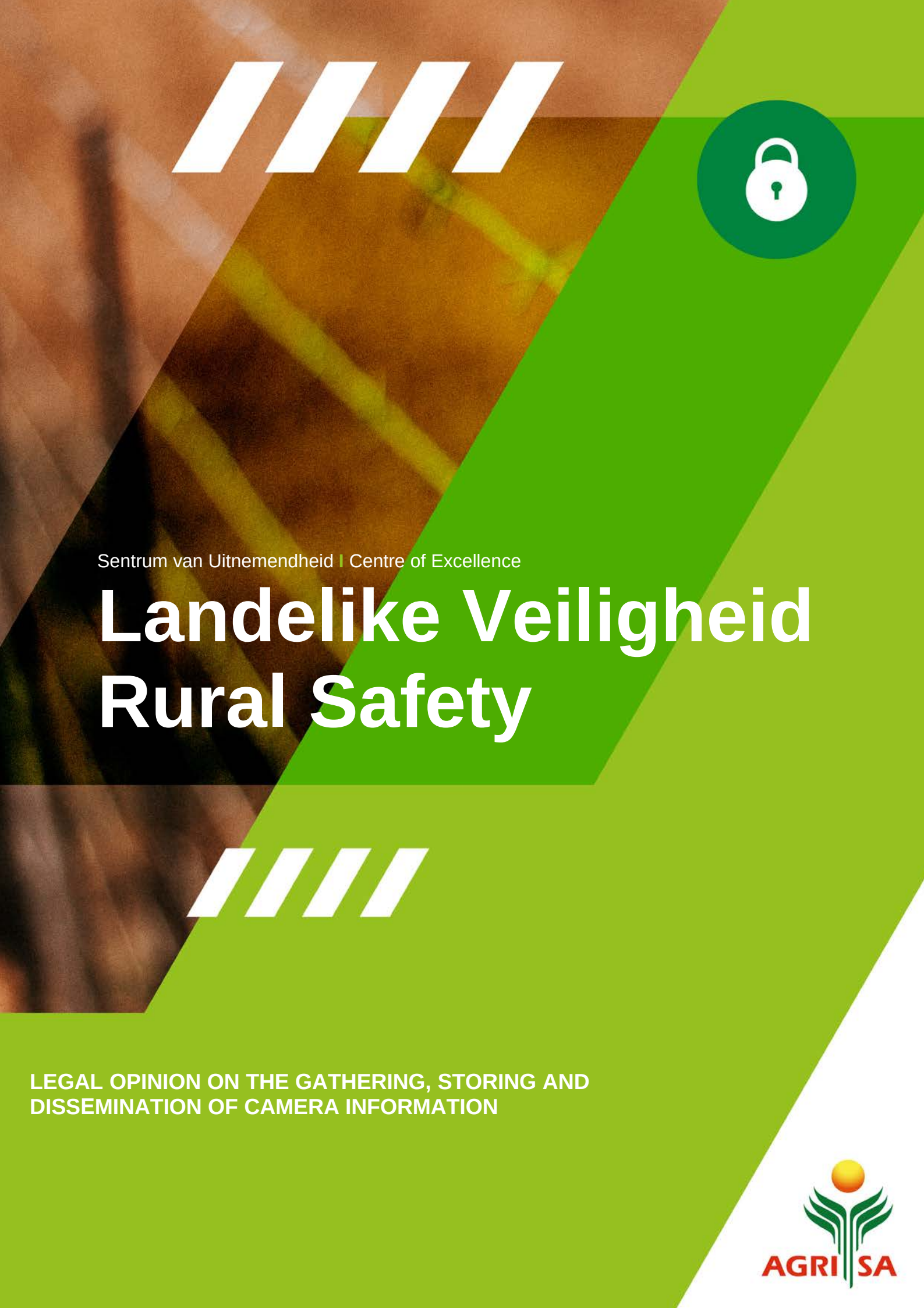

Sentrum van Uitnemendheid I Centre of Excellence

Landelike Veiligheid
Rural Safety

LEGAL OPINION ON THE GATHERING, STORING AND DISSEMINATION OF CAMERA INFORMATION

AGRI SA

LEGAL OPINION ON THE GATHERING, STORING AND DISSEMINATION OF CAMERA INFORMATION

INDEX

HOBSON LEGAL CONSULTING

TAYLOR TORRINGTON INC

To: **Agri SA** **24 August 2022**

Attention: **Kobus Visser**

Email: **kobus@agrisa.co.za**

Dear Mr. Visser

RE: CONSENT TO LIMITED CIRCULATION OF AGRI SA'S POPIA CAMERA SURVEILLANCE OPINION

1. We confirm that we prepared a legal opinion for and on behalf of Agri SA, dated 18 August 2022, entitled: *Re: How Farming Associations Can Legally Store, Use And Disseminate Information Retrieved From Number Plate Recognition Camera Systems (ALPR Cameras) and Other Cameras Erected Along National And Other Road*s (hereinafter referred to as "**the Agri SA Opinion"**)

2. Clause 1.4 of the Agri SA Opinion, provides that the Agri SA Opinion "*may not be relied upon by or disclosed or circulated to, any person or for any other purpose or quoted or referred to in any document or filed with any government or other agency without our prior written consent*."

3. This letter serves to confirm that we consent to Agri SA circulating the Agri SA Opinion, for information purposes and no other purposes, to:

    a) Agri SA's member organisations;
    b) Agri SA' affiliate companies; and
    c) Agri SA's farmer associations.

4. This consent shall in no way be construed as a waiver of any of our rights, nor any extension of any benefit or our liability to any such person (for which we expressly exclude our liability and remain indemnified, to the extent legally permissible).

5. Our rights remain strictly reserved.

Your sincerely

Stormme Hobson

HOBSON LEGAL CONSULTING

TAYLOR TORRINGTON INC

To: **Agri SA** **18 August 2022**

Attention: **Kobus Visser**

Email: **kobus@agrisa.co.za**

Dear Sir

IN RE: HOW FARMING ASSOCIATIONS CAN LEGALLY STORE, USE AND DISSEMINATE INFORMATION RETRIEVED FROM NUMBER PLATE RECOGNITION CAMERA SYSTEMS (ALPR CAMERAS) AND OTHER CAMERAS ERECTED ALONG NATIONAL AND OTHER ROADS

1. **INTRODUCTION**

1.1. We confirm that we have been instructed to prepare this legal opinion for and on behalf of Agri SA (hereinafter referred to as "**Agri SA**").

1.2. The opinions expressed herein are strictly limited to the matters stated in paragraph 3 below and do not extend to any other matters. The opinion is limited to South African law and to the set of facts provided. We accordingly express or imply no opinion on any laws other than those of South Africa and we confirm that we have made no further investigation of any other laws or of any further facts which are not reflected in the documents provided in respect of which our opinion is sought.

1.3. This opinion sets out only those findings which in the professional discretion of the author are relevant to the facts presented. In the circumstances, the potential for undisclosed facts and circumstances exists and the author holds no liability in respect thereof. We furthermore express no view on the validity of the documents (if any) or the facts which we were provided.

1.4. This opinion is addressed to Agri SA and is solely for its benefit. Accordingly, it may not be relied upon by, or disclosed or circulated to, any person or for any other purpose or quoted or referred to in any document or filed with any government or other agency without our prior written consent.

2. **BACKGROUND**

2.1. We have been asked to examine and provide legal advice on how Farming Associations can legally use, store and disseminate information, retrieved from number plate recognition camera systems (ALPR cameras) and other cameras erected along national and other roads ("**Camera Systems**") in terms of the Protection of Information Act 4 of 2013 ("**POPIA/the Act**").

2.2. **All *Capitalised Terms* herein (unless defined in text) should be interpreted in accordance with the meaning attributed to them under POPIA (to the extent applicable).**

2.3. We have been advised that:

a) the South African National Roads Agency SOC ("**SANRAL**"), as the parastatal responsible for the management, control and maintenance of the national road network of South Africa, has concluded an agreement with Agri SA and its nine provincial affiliates (**"SANRAL Agreement**"), to introduce a process whereby Farming Associations can apply for the legal installation of camera systems on national roads, with a view to using such to assist in crime prevention and the tracking down and prosecution of criminals[1];

b) presently, there is a big focus within the farming communities to erect camera systems as a crime deterrent and tracking mechanism to monitor movement in outlying areas and identify suspicious vehicles and persons. The editor of Landbouweekblad on 4 February 2022, wrote; "*The spiderweb security cameras installed across the country have suddenly made rural areas manageable again. Through careful budgeting and with the assistance of Agri SA's Securitas Trust Fund, among others, this has been one of South Africa's greatest successes over the past 20 years*.";

c) the Camera Systems are used to identify suspicious vehicles and persons involved in crime and to assist the police with information, when requested;

d) Farmers also use the Camera Systems to assist in protecting national key points such as the Transnet pipeline running from Durban to Gauteng, through farming land, by identifying suspicious movement on roads near the pipeline and notifying Transnet accordingly; and

e) they also assist farmers to identify veldfires before they spread so that the necessary measures can be taken to contain or extinguish them.

3. For the purpose of this opinion, we will assume (and have accordingly limited and based our opinion on such assumptions) that:

3.1. the Camera Systems in question will all be legally authorised and erected, in terms of the SANRAL Agreement or otherwise;

3.2. the Camera Systems will be owned and operated by the identifiable, formalized or structured Farming Associations;

[1]Agri SA's Procedural Guidelines to deal with applications for the installation of camera systems on national routes, 2021

3.3. the information derived from the Camera Systems is intended to be used, stored and disseminated by the Farming Association for safety, security and crime detection and deterrence purposes;

3.4. the Farming Associations intends to share or give access to the Camera Systems and/or the information derived therefrom to third parties which may include private security companies, the police, individuals, Transnet (or other parastatals) and/or other farming communities and members; and

3.5. the information retrieved by the Camera Systems and intended to be used, stored and disseminated by the Farming Associations may include the following information (collectively or individually defined as **"the Surveillance Information**"):

a) vehicle licence plate registration numbers (in an electronically readable format), along with the make, model and colour of the vehicle;
b) the location of the camera that took the scan;
c) the time and date of image scans and identifying details of the camera that took the scan;
d) images of the person/s in the vehicle (Data Subject/s) passing through the Camera Systems. [We have assumed these will consist of ordinary video images/photograph or "stills" and will not be technologically processed images (such as digitised facial recognition images)][2]; and
e) images/footage of possible or alleged criminal or suspicious behaviour or activities.

4. SCOPE OF THIS OPINION

4.1. This opinion encompasses the following:

a) an overview of the general law around the conflict between the right to privacy versus the right to security (specifically crime prevention, monitoring and tracking) that emanates from the installation and monitoring of camera systems on public roads;
b) guidance on how the Farming Associations can legally store, use and disseminate the Surveillance Information in terms of POPIA; and
c) a Checklist of Action Items for the Farming Association to implement (**See: Annexure A**).[3]

5. THE LAWS GOVERNING CCTV AND OTHER CAMERA SYSTEMS IN SOUTH AFRICA

5.1. CCTV and camera surveillance, in general, is a topical and contentious issue. At its core lies the question of how to balance public safety and security imperatives with the fundamental right to privacy,

[2] If the images will be images that have undergone technical processing, then these may constitute biometric information and will be governed under section 33 of POPIA but arguably still could be justified and permitted on the grounds of "legitimate interest- See: Criminal behaviour
[3] Note this Checklist cannot be read in isolation and must be read with the opinion

as enshrined in Section 14 of the Constitution of the Republic of South Africa. A subsect of the right to privacy even exists, known as: "locational privacy", which refers to the right of individuals to have free and undisturbed or unmonitored movements.[4]

5.2. Globally, there has been a trend towards regulating and putting laws in place when it comes to how people's personal information (and in South Africa also juristic persons' information) is used, monitored and controlled. These are known as data protection laws and in South Africa the primary piece of governing legislation in this regard is POPIA.[5]

5.3. POPIA recognizes the right to privacy. In its Preamble, it even broadens the definition of the right to privacy to include:

'*a right to protection against the unlawful collection, retention, dissemination and use of personal information*.'

5.4. POPIA promotes the protection of Personal Information Processed by public and private bodies by introducing a set of conditions (or minimum requirements) that need to be followed whenever Processing Personal Information. Further it provides for the establishment of an Information Regulator, who is charged with administering the Act and, amongst other things, with issuing codes of conduct or guidelines around information Processing topics and practices.

5.5. To date, no specific guidelines or codes of conduct have been issued relating to the use of camera and CCTV surveillance. This is despite commentary by the Information Regulator that such is under review and imminent[6].

5.6. There have, however, been numerous media reports surrounding the installation of CCTV cameras and automatic licence plate recognition (ALPR) cameras by the likes of Vumacam and in secured complexes and shopping malls[7]. All of which have been brought to the Information Regulator's attention. The release of such a code of conduct therefore appears to be inevitable.

Recommendation:

- **Given the nature of this topic and the media attention, it is evident that the Information Regulator will issue some form of guidance at some stage. When this happens this opinion and the Farming Associations use, store and dissemination of the Surveillance Information should be re-assessed against such guidance.**

[4] J Duncan (2019) UJ's Prof Duncan explores how CCTV surveillance poses a threat to privacy in South Africa, p. 142. Available at: https://www.uj.ac.za/newandevents/Pages/uj-prof-jane-duncanexplores-how-cctv-surveillance-poses-a-threat-to-privacy-in-south-africa.aspx

[5] Depending on the circumstances and context also the Promotion of Access to information Act, 2000("PAIA"), the Cybercrimes Act, 2020 and the Constitution of the Republic of South Africa, amongst others may also apply, these however are generally beyond the scope of this opinion.

[6] https://www.vumacam.co.za/sas-suburban-camera-creep-tests-privacy/

[7] https://www.dailymaverick.co.za/article/2021-09-08-heres-how-johannesburg-security-cameras-track-you/

5.7. Given that there are no current guidelines in place around camera surveillance, the legality of the use, storage and dissemination of the Surveillance Information needs to be assessed against the general provisions of POPIA (as is set out below).

6. POPIA AND CCTV AND OTHER CAMERA SYSTEMS

6.1. POPIA does not contain any specific camera surveillance provisions. Rather it specifies that as from 1 July 2021, all entities must comply with the provisions of POPIA if they engage in the "*Processing*" of "*Personal Information*".

6.2. POPIA defines these two terms as follows:

"***Processing***" as, *inter alia*:

> *any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—*
>
> *(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;*
> *(b) dissemination by means of transmission, distribution or making available in any other form; or*
> *(c) merging, linking, as well as restriction, degradation, erasure or destruction of information.*

"***Personal Information***" as *inter alia*:

> "*information relating to an identifiable living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:*
>
> *(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;*
> *(b) information relating to the education or the medical, financial, criminal or employment history of the person;*
> *(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;*
> *(d) the biometric information of the person;*
> *(e) …;*
> *(f) …;*
> *(g) the views or opinions of another individual about the person; and*
> *(h) the name of the person if it appears with other Personal Information relating to the person.*

6.3. Based on the above, it is evident that the Surveillance Information and the Farming Associations' intended use of the Surveillance Information (as detailed in clause 3.3 and 3.4 above) ("**Intended Surveillance Activities**") would fall within the scope of POPIA and constitute the "Processing" of "Personal Information".

6.4. Camera surveillance generally is regarded as the Processing of Personal Information. To support this conclusion, we have underlined the more pertinent (but not the only) types of Processing activities and categories of Personal Information that would likely be derived during the Intended Surveillance Activities. Further we note that although a single piece of information derived from the Camera Systems about an individual may not be enough to identify the person, if the information can be used in conjunction with other information to identify a person, then it will constitute Personal Information and be subject to the provisions of POPIA.

6.5. Now that we have confirmed that the Intended Surveillance Activities fall under the provisions of POPIA, we need to consider how this will impact on the Farming Associations.

7. APPLICATION OF POPIA

7.1. POPIA is a principle-based (as opposed to rule-based) law. It is centred around 8 principles, referred to as "Conditions", that must be complied with when Processing Personal Information. These Conditions are set out below:

a) Accountability;
b) Processing Limitation;
c) Lawfulness of Processing;
d) Further processing limitation
e) Information Quality;
f) Openness;
g) Security Safeguards; and
h) Data Subject Participation.

7.2. In order to be permitted to engage in the Intended Surveillance Activities the Farming Associations would need to comply with the 8 Conditions.

Condition One: Accountability (Section 8 of POPIA)

7.3. This Condition is essentially a "catch all" condition and provides that when collecting Personal Information from a Data Subject, a Responsible Party (defined below) must ensure that all POPIA principles are complied with.

7.4. POPIA distinguishes between two different types of data processors, namely: Responsible Parties and Operators and imposes different obligations on each.

7.5. Responsible Parties:

a) A Responsible Party is "*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."*

b) Responsible Parties are obliged to comply with all eight POPIA conditions when Processing Personal Information.

c) Analysis: In the current scenario, we have been advised that the Farming Associations will be the owners of the Camera Systems and will determine the purpose (*"the why*") and means ("*the how"*) of Processing the Personal Information. In other words; the purpose the Surveillance Information collected is for, what it will be used for, who it will be shared with and how it will be recorded, stored, saved is all determined by the Farming Associations. It is therefore evident that the Farming Associations would constitute a Responsible Party in this current situation.

d) If at any stage, any of the Farming Associations (which includes any person or body under its direct control) are no longer the owners of the Camera Systems or no longer determine the purpose and means for the Processing of the Personal Information, then this position would need to be re-considered.

e) Further it is worth noting that the relationship and information sharing with Transnet and the police, is a bit more complicated. Ultimately this does not appear to alter the position of the Farming Association as a Responsible Party. It may, however, introduce additional key players into the Intended Surveillance Activities and give rise to potential Joint Responsible Party or Operators relationships. We recommend that the Faming Associations, try to enter into a Memorandum of Agreement with the Transet and/or the police regarding such information exchanges in order to better cement the position. This is not mandatory but could assist in justifying the information sharing as being viewed as an obligation imposed by law [8] or could justify any further Processing as being necessary to comply with an obligation imposed by law.[9]

7.6. Operators:

a) An Operator is as: "*a person who processes personal information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that party*." This would generally include third party service providers or any other party, who acts on behalf of or fulfils the instructions of a Responsible Party. Operators do not determine the purpose (the "*why*") or means (the "*how*") by which the Personal Information is Processed, they merely execute the Responsible Party's objective/instructions.

b) Unlike Responsible Parties, Operators are only required to comply with the seventh condition of POPIA, relating to security safeguards. This is because Operators are seen to act on behalf of

[8] Section 11 of POPIA
[9] Section 15 (c) of POPIA

Responsible Parties, who ultimately still remain responsible for ensuring the continued protection of the Personal Information even when it is passed to third parties.

c) Analysis: In this case, we have been advised that the Farming Associations will share the Surveillance Information with third parties, such as security providers. This means that the Farming Associations would also have to implement measures (including contractual measures) to ensure that all of their third-party providers also comply with POPIA when Processing information from the Camera Systems.

Recommendations:

Each Farming Association must:

- ***implement (or supplement existing) data compliance measures (policies, practices and procedures) relating to the Intended Surveillance Activities to ensure such comply with the 8 conditions;***
- ***identify all third-party providers that it shares Personal Information with or who assists it with the Camera System surveillance and/or the Surveillance Information (e.g. security companies, software providers etc) and put Operator Agreements in place with each.***

Condition Two: Processing Limitation (Sections 9-12 of POPIA)

7.7. This Condition requires that in order for the Farming Associations Intended Surveillance Activities to be permitted, the (Personal) Surveillance Information would have to be:

a) processed lawfully and not infringe the privacy of the Data Subject;

b) processed for a purpose that it is adequate, relevant and not excessive (the principle of "minimality");

c) processed in the case of consent or a justified reason, which includes:

i. a contract with the Data Subject;

ii. an obligation imposed by law;

iii. the legitimate interest of the Data Subject; or

iv. if the Processing is necessary for pursuing the legitimate interests of the Responsible Party or of a third party to whom the information is supplied ; and

d) collected directly from the Data Subject, subject to certain exceptions, which includes:

i. maintaining the legitimate interests of the Responsible Party or of a third party to whom the information is supplied;

ii. compliance would prejudice a lawful purpose of the collection; or

iii. compliance is not reasonably practicable in the circumstances of the particular case.

(emphasis added)

7.8. In this scenario, the Farming Associations reason (and intended purpose) for collecting the Surveillance Information is a crime detection and deterrence mechanism and to protect the safety and security of the farming communities/areas and broader public **("Intended Security Purpose").**

7.9. This would constitute Processing "*necessary for pursuing the legitimate interests of the (Farming Association) or a third party to whom the information is supplied*",

7.10. This is a sufficient ground for the allowance of the Intended Surveillance Activities, provided that the Farming Associations implement and maintain other related compliance (Processing Limitation) measures when dealing with the Surveillance Information and Intended Surveillance Activities.

7.11. These would include:

a) implementing a POPIA/Privacy Policy (and various related policy/ies and procedures) that:

i. outlines the specific purpose of the Camera System surveillance and the purpose for which (Personal) Surveillance Information will be used (this is critical in justifying the use of the Camera System and justifying that they are being used for a "*legitimate interest*";
ii. details the rules and restrictions in place relating to the access to and sharing of the Surveillance Information; and
iii. provides for POPIA centric training to anyone who will have direct access to the Camera Systems or is involved in using, storing, disseminating or sharing the information;

b) implementing rules that the Camera Systems may only be used to fulfil the Intended Security Purpose and not for any other non-related purposes (e.g. for any personal, social or commercial purposes);

c) only collecting/using the absolute minimum Personal Information required to fulfil the Intended Security Purpose and nothing that is excessive or superfluous. To this end, the placement of Camera Systems should be strategic and aligned with the Intended Security Purpose. They should be positioned in areas where they will capture security breaches (and not, for example, to spy on people). The norm in most common law jurisdictions is that there is no reasonable expectation of privacy in public spaces. So, camera systems in and surveillance of access points and common areas will likely be permissible. Camera Systems in other areas (i.e. outside of common areas or access points) however, should only be erected if it can be shown that a person would have no reasonable expectation of privacy and that the surveillance can be linked back to the Intended Security Purpose. i.e. has been installed to maximize security;

d) making the public/Data Subjects aware and warn them that the area is monitored by camera surveillance in order to reduce their expectation of privacy. In this regard it is recommended that

signage be placed in areas where cameras are operating. A sign which identifies that the area is monitored by cameras together with a link to the POPIA Policy, is recommended.

Recommendations:

Each Farming Association should

- ***Implement a Privacy Policy[10] (which is made available on its website), outlining:***
  - ***what information is collected by the Camera Systems (which should be minimal);***
  - ***who it is collected by;***
  - ***for what purpose; and***
  - ***all other general rules and restrictions relating to the Processing, storage and use of the information***
- ***Ensure the Surveillance activities are only use for the Intended Security Purpose – not any other purpose***
- ***Restrict who has access and how shared (give training)***
- ***Collect only what is necessary – place camera in strategic places***
- ***Signage: Putting up a sign/s next and around the area monitored by the Camera Systems and identifying where more information on the purpose for such surveillance can be found. E.g.***

"This area is monitored by camera surveillance primarily for safety, security and crime prevention and detection purposes. For more information visit [insert website or other address].

Condition Three: Purpose Specification (Section 13-14 of POPIA)

7.12. Under this Condition when engaging in the Intended Surveillance Activities, the Farming Association would have to ensure that:

a) The Personal Information that they Process is only collected for a specific, explicitly defined & lawful purpose that is related to a function or activity of the Responsible Party (Farming Association); and

b) Records of Personal Information are not retained for longer than required to fulfil the purpose.

Defined and lawful purpose related to a function or activity of the Responsible Party

7.13. In terms of this Conditions, you are only permitted to engage in the collection of Personal Information if such is lawful and the purpose for the collection is related to one of your specific functions or activities. Given the general nature of Farming Associations, which is to oversee and protect the interests of the broader and designated farming community; the installing of Camera Systems in order to protect and promote the safety of these communities (and to protect the broader public interest in the case of the Transnet line) would clearly be related to a function or activity of the Farming Associations.

7.14. Secondly the Processing must be shown to align with the legal principles of necessity and proportionality. In this case, you need to be able to demonstrate that the limitation (on the right to

[10] If there is already a Privacy Policy in place this can be supplemented to the extent noted

unfettered privacy) meets a '*pressing social need*' and is proportionate to the legitimate aim that is being pursued. [11]

7.15. In South Africa, as in other jurisdictions, the general objective of installing surveillance cameras is public safety and security. But in South Africa, more emphasis is placed on such Camera Systems for crime prevention and personal/communal security. Considering the high levels of crime in South Africa, one could say crime reduction is a pressing social need[12]. There is a strong but untested belief among policymakers, private security companies and marketers of camera technologies that Camera Systems can detect, deter and even prevent crime which is seen as creating a multiplier effect on policing resources.

7.16. This position is not definitive, however, in our view, given the high levels of crime in South Africa, security, crime detection and crime deterrents would be regarded as a specific and lawful purpose.

Retention of records

7.17. The other requirement under this Condition is that Personal Information should not be retained for longer than is necessary to achieve the purpose for which it was collected.

7.18. There is no definitive period for how long Personal Information should be retained for, as this will always depend on and relate back to the period that is *"required to fulfil the purpose".* The period however will always have to be reasonably justifiable.

7.19. In the course of the Intended Surveillance Activities, the Farming Associations will Process multiple Data Subject's Personal Information. However not all of this information will be (or remain) relevant for the Intended Security Purpose. In fact a lot of the information collected may not relate back to any potential security, public or criminal threat or behaviour at all (e.g. camera surveillance of an ordinary person who is just a "passer- by")

7.20. In instances, where the Farming Association is holding Personal Information about Data Subject that is not relevant for the Intended Security Purpose, then such information should be destroyed as soon as it is no longer needed.

7.21. VumaCam, for example, who similarly owns ALPR camera systems for (commercial but also indirect) security related purposes, only stores its records of number plates for a period of 30 days. This is a

[11] A Minnaar (2012) Private security companies, neighbourhood watches and the use of CCTV surveillance in residential neighbourhoods: the case of Pretoria East, Acta Criminologica: Southern African Journal of Criminology, Special Edition 1, 2012

[12] J Duncan (2019) UJ's Prof Duncan explores how CCTV surveillance poses threat to privacy in South Africa, p. 142. Available at: https://www.uj.ac.za/newandevents/Pages/uj-prof-jane-duncanexplores-how-cctv-surveillance-poses-a-threat-to-privacy-in-south-africa.aspx

good yard stick in assessing what would be considered a “reasonable” period for retaining information that does not link back to the Intended Security Purpose.

7.22. That said, the storage period and what would be reasonable may fluctuate based on various factors. For instance, records pertaining to any vehicles of interest or suspicious vehicles or persons, could arguably be stored for longer periods.

7.23. Note: there are exceptions to this rule, for example, if the information is being retained for purposes of historical, statistical or research purposes where a law requires a longer retention period or where a party has consented, or contractually agreed, to the longer retention period.

Recommendations

- ***Ensure the Camera Surveillance is only carried out for the Intended Security Purpose and <u>not</u> any other purpose***
- ***Put retention measures, policies and practices in place for the storage the Personal (Surveillance) Information and store Surveillance information ONLY for as long as the purpose for which it is recorded requires .***

Condition Four: Further Processing Limitation (Section 15 of POPIA)

7.24. This Condition prescribes, that a Data Subject’s Personal Information may not be further processed in any way that is incompatible with the purpose for which the Personal Information was initially collected.

7.25. In this case, the Farming Association is collecting the Surveillance Information for the Intended Security Purpose. All Processing (use or onward sharing) of the information should therefore always be for a purpose that is related back to the Intended Security Purpose and not used for any other purposes (i.e. personal or commercial reasons).

7.26. Access and sharing of the information with any third parties should therefore be done on a limited or restricted basis and handled with caution based on its compatibility with the Intended Security Purpose.

7.27. Section 15 sets out criteria for what generally would be regarded as “compatible” and what would not as well as express exceptions to this requirement. Such examples are where consent is obtained or the further Processing of the information is necessary to prevent or mitigate a serious and imminent threat to public safety, which in the given scenario may be a common occurrence.

7.28. Further when it comes to further Processing, each specific instance should be evaluated to ensure that the use of the Personal Information is justifiably reasonable in terms of the instance. For example, if a suspicious vehicle or individual is identified by the Camera System and poses an imminent threat, it

would be reasonably justifiable for the Farming Association to notify third parties immediately and to pass on the Personal Information (number plate and description of persons).

Recommendations

- ***Third parties should not be given unfettered access to the Camera Systems;***
- ***Sharing of information with any third parties should also be limited;***
- ***Put policies and rules in place relating to who information can be shared with and/or for what it can be used.***
- ***All third parties who access the systems should sign POPIA centric agreements and undergo POPIA training.***

Condition Five: Information Quality (Section 16 of POPIA)

7.29. This Condition requires that all Personal Information held by the Farming Associations should be complete, not misleading, up to date and accurate. To this end, the Farming Associations should implement various mechanisms to ensure that the information that they hold and more specifically that they retain is accurate and up to date.

7.30. There are various measures the Farming Association could implement to ensure this, such as regular audits. They can include provision in their Privacy Policy for Data Subjects to update their Personal Information

Recommendation:

- ***the Farming Associations should implement various mechanisms to ensure that the information that they hold and more specifically that they retain is accurate and up to date.***

Condition Six: Openness (Section 17 and 18 of POPIA)

7.31. Under this Condition, the Farming Associations must take reasonably practicable steps to ensure that all Data Subjects, whose information is collected as part of the Surveillance Activities, are aware of:

a) the fact that their Personal Information is being collected and stored;
b) the name and contact details of the entity/association collecting the information;
c) the purpose for which it is being collected;
d) whether or not the supply of the information by the applicant is voluntary or mandatory and the consequences of failure to provide the relevant information;
e) where the collection of information is authorised or required under any law and the particular law to which the collection is subject; and
f) whether the responsible party intends to transfer the information to a third country or international organisation and the level of protection of that information.

Recommendations;

- **Erect signage in and around the surveillance areas making the general public/Data Subjects aware of the fact that the area is under camera surveillance and where they can find more information on what is done with their information; and**
- **Publish Privacy Policy outlining details on the Surveillance Activities and all related Processing.**

Condition Seven: Security Safeguards (Section 19- and 20 and 21 and 22 for Operators)

7.32. This Condition requires the Farming Associations to implement technical and organizational measures across all levels to secure the integrity of Personal Information, and to guard against the risk of loss, damage or destruction of Personal Information.

7.33. It also sets out the requirements that must be followed when there are reasonable grounds to believe that the Personal Information of a Data Subject have been accessed by any unauthorized person. The Farming Association should have set policies and procedures in place that address how such a data breach will be handled. For example what should happen in the event that the Surveillance Information falls into "the wrongs hands", either negligently or through a cyber-attack or hack etc.

7.34. To this end the Farming Associations will have to ensure that all Personal Information that is collected is secured by systems that have high levels of data security, vetting, training, log-ins and VPN for traceability and furthermore systems must be in place to audit activity on the Camera System.

7.35. Further they will be obliged, in terms of a written contract between it and any third-party service provider ensure that such third party establishes and maintains the security measures that it is required to have in place when Processing

Recommendation:

- ***Implement Security Safeguards to prevent unauthorised access by implementing appropriate, reasonable, technical and organisational measures to prevent data breaches***

Condition Eight: Data Subject Participation (Sections 23 and 24)

7.36. The last Condition prescribes that Data Subjects are entitled to request the Farming Associations to provide them with the particulars of their Personal Information that are held by the Farming Association as well as to the identity of any entity or person that has had access to their Personal Information. The Data Subject is also entitled to require the correction or destruction/deletion of any information held by the Farming Association to the extent that there is no lawful reason for such request to be declined.

7.37. This can be dealt with in a Privacy Policy.

Recommendations

- **Privacy Policy to be implemented or updated to cover the above; and**
- **PAIA Manual also to be implemented or updated[13].**

8. ADDITONAL CONSIDERATIONS IN RELATION TO SPECIAL (CRIMINAL BEHAVIOUR) AND MINORS' PERSONAL INFORMATION

8.1. In addition to the above general Conditions, POPIA also contains additional obligations and limitations when it comes to the Processing of certain Personal Information that is regarded to be "special" or more sensitive in nature.

8.2. This includes information:

a) concerning a Data Subject's criminal behaviour (which includes the alleged commission by a Data Subject of any offence); and

b) minor/children's information.

8.3. In these instances there are additional limitations and restrictions on a party's ability to Process this information and so the Farming Associations should adopt additional precautionary practices and measures in these instances. For example, additional security measures or restrictions be implemented once criminal behaviour or a minor's information has been identified.

8.4. In the case of criminal behaviour; there is a high probability that the Farming Associations will Process this type of information on a regular basis, given that this information links back to the very Intended Security Purpose that the surveillance is intended for.

8.5. To this end, it becomes even more critical that that the Farming Association only use legally authorised and erected Camera Systems, comply all 8 Conditions of POPIA and only use the Surveillance Information for the Intended Security Purposes. If they do so it will support in justifying an exception to this rule under section 27 of POPIA and the contention that they "*obtained that information in accordance with the law*" and that the Processing of the information is being used for a "*legitimate and lawful purpose".*

8.6. In the case of minor/children's Information, there is a strong probability that the Personal Information of children could be processed, for example if an image is recorded on the Camera Systems. In these cases, it is recommended that the Farming Associations, delete any Personal Information relating to

[13] See Information Regulator website for a template PAIA Manual. PAIA regulates "access to information" and seeks to give people freedom to information (including but not limited to personal information- provided such does not conflict with POPIA).

children as soon as is reasonably possible (unless such may relate back to, for example, a security incident).

9. CONCLUSION

9.1. The use of camera and CCTV surveillance is a sensitive topic from both a legal and societal perspective and should be treated with caution.

9.2. That said, the Farming Associations would be entitled to use, store and disseminate the Surveillance Information from the Camera Systems, provided that they can illustrate that such is necessary to pursue their legitimate interests.

9.3. In the current scenario, the Surveillance Information is intended to be used for the lawful purpose of detecting, tracking and preventing crime and ensuring the safety and security of the broader community and would be permitted on the basis of being in their legitimate interests, provided that they comply with the 8 Conditions of POPIA.

9.4. Under these Conditions, the Farming Community would have to:

a) adopt the principle of “minimality” by only monitoring the information that is necessary to fulfil their Intended Security Purpose. This would include limiting the Personal Information that they collect to what is absolutely necessary and only surveying essential or key security areas/locations;
b) notify the public/persons that the areas are under camera surveillance by erecting prominent signage at the locations that are being monitored;
c) ensure that the Surveillance Information is only used and kept in order to fulfil the Intended Security Purpose;
d) restrict access to the Camera Systems and Surveillance Information to authorised persons that require the Information for the Intended Security Purpose;
e) implement measures to ensure that Personal Information is only stored for as long as the purpose for which it is recorded required, otherwise it must be deleted; and
f) implement security safeguards to protect the Personal Information and to prevent data breaches.

ANNEXURE A

FARMING ASSOCIATION CAMERA SYSTEM CHECKLIST

	ACTION	STATUS
1.	All Camera Systems should be legally erected and authorised in terms of the SANRAL Agreement or otherwise.	
2.	If/when any guidelines (i.e. a code of conduct) on CCTV or camera surveillance is issued by the South African Information Regulator (which it seems is evident) or any other public authority in the future, the Farming Associations should update and re-assess their use, store and disseminate of the Surveillance Information against such guidelines.[14]	
3.	Implement (or supplement any existing) data compliance policies, practices and procedures to cater for the camera surveillance, all related activities and the sharing of any Surveillance Information (see further details/guidance on this below).	
4.	Ensure the camera surveillance is only carried out for the intended purpose, i.e., safety, security, crime detection and deterrence- ("**Intended Security Purpose**") and **not** any other purpose e.g., personal or commercial purposes (*spying on people, reporting people's social/personal movements etc.*)	
5.	Only collect/process minimal (Personal) Information and nothing excessive. Collect as little information as is needed to fulfill the Intended Security Purpose.	
6.	Place Camera Systems in strategic places/areas: a) Where possible in open, common and public spaces; and b) Where the Intended Security Purpose can be maximised (e.g., high-risk areas or areas that will maximise crime detection or deterrence)	
7.	Notify the public/data subjects that an area is monitored by camera surveillance and the purpose of the surveillance. This can be done by putting up a sign/s next and around the area monitored by the Camera Systems and noting where more information on the purpose of the surveillance can be found. E.g. *"This area is monitored by camera surveillance primarily for safety, security and crime prevention and detection purposes. For more information visit XXX [insert website or other address].*	
8.	Publish (or supplement any existing) Privacy Policy to cover the camera surveillance activities and make this available to the public (e.g., on your website and at your local offices). The Policy should state: a) the fact that Personal Information is being collected and stored by the Camera Systems; b) what information is being collected on the Camera Systems; c) the number and location of the Camera Systems; d) the name and contact details of the Farming Association (or any other entity/association) collecting the information; e) the purpose for which the information is being collected (the Intended Security Purpose); f) the operation times of the video surveillance system; g) the length of time video footage is retained and how it is securely stored; h) whether or not the supply of the information is voluntary or mandatory and the consequences of failure to provide the relevant information;	

[14] This note is included as it has been stated in the media that the publication of a Code of Conduct on Surveillance is anticipated. When this happens, we do not anticipate any big changes but sometimes additional obligations or practical tips are detailed in these Guidance notes/Codes of Conduct and so they must be reviewed.

	i) where the collection of information is authorised or required under any law and the particular law to which the collection is subject; j) whether the Farming Association intends to transfer the information to a third country or international organisation and the level of protection of that information; and k) outline the Data Subjects rights (i.e., to object, have their information erased, contact the Regulator etc.)	
9.	Restrict access to the Camera Systems and the information retrieved on the camera systems to a limited number of authorized people.	
10.	Put retention measures, policies and practices in place for the storage and deletion of all Surveillance (Personal) Information. ONLY store Surveillance Information for as long as it is required (i.e., for as long as it is still needed for security related purposes. Where information is no longer needed or necessary for security purposes it must be deleted. Guidance: delete all unnecessary information, which is not critical and which does not relate back to any Intended Security Purpose as soon as possible- work on 30 days as a guide. e.g., *surveillance of ordinary "passers-by"* Information that is relevant, i.e., relates back to the Intended Security Purposes, can be retained for longer periods e.g., *footage of a suspicious act or an actual criminal occurrence.*	
11.	Implement security safeguards on the camera and information systems and to prevent unauthorised access to the system, by implementing appropriate, reasonable, technical and organisational measures to prevent data breaches. (e.g., password protections, encryptions etc.).	
12.	Identify all third-party providers that you will shares the Surveillance (Personal) Information with or who assists you with the Camera System surveillance and/or the Surveillance Information (e.g., security companies, software providers etc.) and put Operator Agreements in place with each.	

ANNEXURE A

FARMING ASSOCIATION CAMERA SYSTEM CHECKLIST[1]

	ACTION	STATUS
1.	All Camera Systems should be legally erected and authorised in terms of the SANRAL Agreement or otherwise.	
2.	If/when any guidelines (i.e. a code of conduct) on CCTV or camera surveillance is issued by the South African Information Regulator (which it seems is evident) or any other public authority in the future, the Farming Associations should update and re-assess their use, store and disseminate of the Surveillance Information against such guidelines.[2]	
3.	Implement (or supplement any existing) data compliance policies, practices and procedures to cater for the camera surveillance, all related activities and the sharing of any Surveillance Information (see further details/guidance on this below).	
4.	Ensure the camera surveillance is only carried out for the intended purpose, i.e., safety, security, crime detection and deterrence- ("**Intended Security Purpose**") and **not** any other purpose e.g., personal or commercial purposes (*spying on people, reporting people's social/personal movements etc.*)	
5.	Only collect/process minimal (Personal) Information and nothing excessive. Collect as little information as is needed to fulfill the Intended Security Purpose.	
6.	Place Camera Systems in strategic places/areas: a) Where possible in open, common and public spaces; and b) Where the Intended Security Purpose can be maximised (e.g., high-risk areas or areas that will maximise crime detection or deterrence)	
7.	Notify the public/data subjects that an area is monitored by camera surveillance and the purpose of the surveillance. This can be done by putting up a sign/s next and around the area monitored by the Camera Systems and noting where more information on the purpose of the surveillance can be found. E.g. *"This area is monitored by camera surveillance primarily for safety, security and crime prevention and detection purposes. For more information visit XXX [insert website or other address].*	
8.	Publish (or supplement any existing) Privacy Policy to cover the camera surveillance activities and make this available to the public (e.g., on your website and at your local offices).	

[1] To be read in conjunction with Agri SA opinion dated 18 August 2022
[2] This note is included as it has been stated in the media that the publication of a Code of Conduct on Surveillance is anticipated. When this happens, we do not anticipate any big changes but sometimes additional obligations or practical tips are detailed in these Guidance notes/Codes of Conduct and so they must be reviewed.

	The Policy should state: a) the fact that Personal Information is being collected and stored by the Camera Systems; b) what information is being collected on the Camera Systems; c) the number and location of the Camera Systems; d) the name and contact details of the Farming Association (or any other entity/association) collecting the information; e) the purpose for which the information is being collected (the Intended Security Purpose); f) the operation times of the video surveillance system; g) the length of time video footage is retained and how it is securely stored; h) whether or not the supply of the information is voluntary or mandatory and the consequences of failure to provide the relevant information; i) where the collection of information is authorised or required under any law and the particular law to which the collection is subject; j) whether the Farming Association intends to transfer the information to a third country or international organisation and the level of protection of that information; and k) outline the Data Subjects rights (i.e., to object, have their information erased, contact the Regulator etc.)	
9.	Restrict access to the Camera Systems and the information retrieved on the camera systems to a limited number of authorized people.	
10.	Put retention measures, policies and practices in place for the storage and deletion of all Surveillance (Personal) Information. ONLY store Surveillance Information for as long as it is required (i.e., for as long as it is still needed for security related purposes. Where information is no longer needed or necessary for security purposes it must be deleted. Guidance: delete all unnecessary information, which is not critical and which does not relate back to any Intended Security Purpose as soon as possible- work on 30 days as a guide. e.g., *surveillance of ordinary "passers-by"* Information that is relevant, i.e., relates back to the Intended Security Purposes, can be retained for longer periods e.g., *footage of a suspicious act or an actual criminal occurrence.*	
11.	Implement security safeguards on the camera and information systems and to prevent unauthorised access to the system, by implementing appropriate, reasonable, technical and organisational measures to prevent data breaches. (e.g., password protections, encryptions etc.).	
12.	Identify all third-party providers that you will shares the Surveillance (Personal) Information with or who assists you with the Camera System surveillance and/or the Surveillance Information (e.g., security companies, software providers etc.) and put Operator Agreements in place with each.	