National Farmers Federation

Australian Farm Data Code

Best Practice Guide

Edition 1

7 June 2023

Contents

Introduction

This guide should be read in conjunction with the Australian Farm Data Code v2 (the Code).

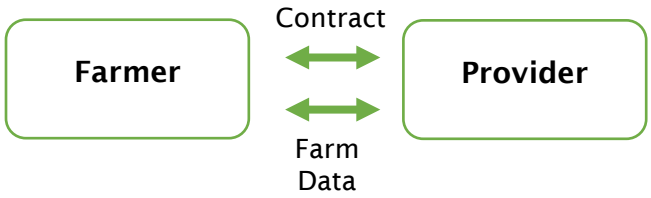
The purpose of this guide is to provide guidance and suggestions on the how the principles of the Code can be practically implemented. It will help Providers give Farmers an excellent experience that will build trust in the data management practices of the Provider.

Definitions

Please refer to the Code for the latest definitions of terms used in this context, most importantly the definition of Farm Data.

Compliance with the Code for Providers with a direct contractual relationship with Farmers

The Code is currently focussed on Providers handling Farm Data, with a direct contractual relationship with Farmers. The Code can be read as-is for this scenario.



Compliance with the Code for downstream Providers that handle Farm Data without a direct contractual relationship with Farmers

The Code is currently focussed on Providers handling Farm Data, with a direct contractual relationship with Farmers, however compliance with the Code is encouraged for all Providers handling Farm Data.

To apply the Code to such downstream entities, the Code needs to be interpreted from a specific perspective. This section provides guidance on how this interpretation should be made.

Please note that the application of the Code for this scenario has not yet been tested with real-world examples as at Mar '23, so this is preliminary advice only – please contact us at farmdatacode@nff.org.au for the most up to date advice.

Before granting access to Farm Data to the third party (Provider B), Provider A should ensure that a contract exists with Provider B that reflects equivalent terms for Farm Data management as those agreed with the Farmer.

The downstream Provider B is then the third party to the contract between the Farmer and their direct Provider A.

To apply the Code to such a scenario the following interpretation is required:

- **Principle 1.1:** The contract between Provider A and Provider B needs to be reconciled to the original contract between Provider A and the Farmer, to ensure data related terms are at least as favourable to Farmers. A similar reconciliation of data management practices against the Code should also be carried out. The same (or more favourable) terms and data management practices should apply to Farm Data as it flows down the supply chain. Risks or detriments that may affect Farmers should be fed back up the supply chain to Farmers from downstream entities.

- **Principle 1.2:** Provider A should get fully informed and express consent from the Farmer for the contract terms, and then Provider A should provide fully informed and express consent to Provider B's terms (which should be equivalent or more favourable to Farmers).

- **Principle 1.3-1.4:** Notification of, and changes to Provider B's terms, need to flow back up the supply chain to Provider A and then onto the Farmer, via respective contracts. If the Farmer does not consent to the changes in Provider A's terms, then Provider A should not accept the changes to Provider B's terms.

- **Principle 1.5:** Provider B could provide a way for Farmers to contact them directly or via Provider A.

- **Principle 1.6:** Provider B can communicate to Farmers directly or via Provider A.

- **Principle 2.1:** If Provider B is using Farm Data to create any value, value should flow back to the Farmer either directly or via Provider A.

- **Principle 2.2:** Provider B can communicate to Farmers directly or via Provider A.

- **Principle 3.1:** Farmers agree to parties with whom data is shared, through contract terms. The third parties that Provider B wants to share Farm Data with should be specified in the contract between Provider A and Provider B, and be communicated to the Farmer via Provider A. Parties nominated by Farmers to access Farm Data should be either able to get Farm Data directly from Provider B or via Provider A (note that contract between Provider A and Provider B should allow for this).

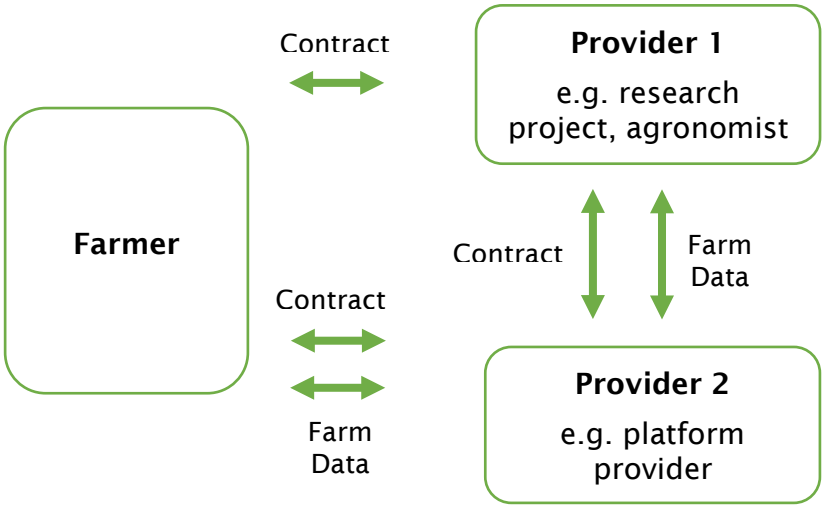
- **Principle 3.2:** Compliance to the Code and the contract terms between Provider A and the Farmer should flow through the supply chain to all downstream Providers.

- **Principle 3.3:** Provider B could provide a way for Farmers to contact them directly or via Provider A (note that contract between Provider A and Provider B should allow for this).
- **Principle 3.4:** Provider B can communicate to Farmers directly or via Provider A (note that contract between Provider A and Provider B should allow for this).
- **Principle 3.5:** Provider B can communicate to Farmers directly or via Provider A (note that contract between Provider A and Provider B should allow for this).
- **Principle 4.1:** Farmers should be able to request this directly from Provider B or via Provider A (note that contract between Provider A and Provider B should allow for this).
- **Principle 4.2:** This principle can be applied as is.
- **Principle 4.3:** Farmers should be able to request this directly from Provider B or via Provider A (note that contract between Provider A and Provider B should allow for this).
- **Principle 4.4:** Farmers should be able to request this directly from Provider B or via Provider A (note that contract between Provider A and Provider B should allow for this).
- **Principle 4.5:** Provider B can communicate to Farmers directly or via Provider A (note that contract between Provider A and Provider B should allow for this).
- **Principle 4.6:** Farmers should be able to request this directly from Provider B or via Provider A (note that contract between Provider A and Provider B should allow for this). In this principle 'service termination' should include the termination of the contractual relationship between the Farmer and Provider A, as well as the termination of the contractual relationship between Provider A and Provider B.
- **Principle 5.1:** This principle can be applied as is.
- **Principle 5.2:** This principle can be applied as is.
- **Principle 5.3:** Provider B can communicate to Farmers directly or via Provider A (note that contract between Provider A and Provider B should allow for this).
- **Principle 5.4:** This principle can be applied as is.
- **Principle 5.5:** This principle can be applied as is.
- **Principle 6.1:** This principle can be applied as is.
- **Principle 6.2:** This principle can be applied as is.
- **Principle 6.3:** Provider B can communicate to Farmers directly or via Provider A (note that contract between Provider A and Provider B should allow for this).

Compliance with the Code when there are multiple Providers that handle Farm Data in a direct contractual relationship with Farmers (and possibly each other)

There are scenarios where the Farmer is agreeing to multiple sets of terms: terms of the Provider of the platform they are putting their Farm Data into, and terms of the Provider that is getting access to the data e.g. for research purposes, or for the purpose of providing a service like agronomy.

Please note that the application of the Code for this scenario has not yet been tested with real-world examples as at Mar '23, so this is preliminary advice only – please contact us at farmdatacode@nff.org.au for the most up to date advice.



As the Farmer has a direct contract with both Providers, Provider 1 who is receiving the data from the platform provider Provider 2, is considered to be nominated by the Farmer (as opposed to a third party nominated by Provider 2 e.g. advertising companies).

Both Providers should be complying with the Code as they are handling Farm Data.

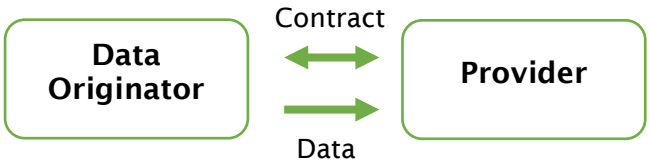
In this case, as the Farmer has **chosen** to consent to a contract with each Provider, under Principle 3.2, Provider 2 does not have a responsibly to ensure that Provider 1 complies with the Code, and vice versa.

However, if Provider 1 has not been nominated by the farmer, but instead is actually a secondary Provider that the farmer **has to** deal with in order to use the product/service, then Provider 2 has a duty to ensure Provider 2 complies with the Code under Principle 3.2.

Compliance with the Code for Providers that do not handle Farm Data but want to apply the Code

The Code is currently focussed on Providers handling Farm Data, who have a direct contractual relationship with Farmers, however the Code can be extended to guide data terms and policies between any parties and for any data.

Please note that the application of the Code for this scenario has not yet been tested with real-world examples as at Mar '23, so this is preliminary advice only – please contact us at farmdatacode@nff.org.au for the most up to date advice.



Assuming that there is a contractual relationship between two entities, one supplying the data, and one receiving it, and only non-Farm Data is in scope, to apply the Code to such a scenario simply:

- replace 'Farmer' with 'Data Originator' (the party providing the data)
- replace 'Farm Data' with the data in scope (ensure it is well defined first)

There may also be other parties involved e.g. data processors, who may be a third party to any contract between the Data Originator and Data Recipient.

Guidance for Code Principles

Principle 1: Transparency

Transparent, clear and honest collection, use and sharing of Farm Data.

Principle 1.1

Providers will:

Provide Farmers with plain-English, easily found terms and associated policies for data collection, use, and sharing detailing:

- the identity of the contracting party/ies;
- what Farm Data and any other data about the Farmer or their farm/business, will be collected, created, aggregated, used, or shared;
- purpose/s for which Farm Data and any other data about the Farmer or their farm/business is being collected, used and shared;
- the value being created for the Farmer, and the Provider;
- how Farm Data will be managed and shared, in terms of security, access, and de-identification protocols;
- identity and/or nature of any other entities with whom it shares Farm Data;
- processes and conditions for data retention, data retrieval, and service termination; and,
- any risks or detriments that may adversely affect Farmers who share data with the Provider.

Best practice for principle 1.1

Data sharing terms need to be legally binding e.g. a contract, terms and conditions, or an End User Licence Agreement.

In addition to addressing the points listed in principle 1.1, the terms should:

- Use language that a high school student would understand – use an app like https://hemingwayapp.com/ to test the readability score
- Be accessible:
- Minimum 10pt font with option to enlarge on screens
- High contrast, so at least 4:5:1 exists between text (and images of text) and background behind the text
- Web-based terms should comply with Web Content Accessibility Guidelines (WCAG)
- Avoid legal/industry jargon and acronyms where possible

- Be concise - use short sentences and smaller paragraphs
- Specify high level data types e.g. soil data
- Be clear about what is original Farm Data, the processed/transformed version of that Farm Data, and any new data (e.g. insights, interpretations, recommendation) created by the Provider based off the Farm Data
- Specify purpose per data type. E.g. aggregation to create benchmarking reports, derive new data, improve the product, Provider's advertising or marketing, product personalisation, app functionality, account management, communications (e.g. newsletter), fraud prevention/security, compliance
- Specify the value the Farmer is getting (e.g. product improvements, discounts, reports or recommendations, getting Farm Data from up the supply chain)
- Reference specific legislation and policies with links where relevant e.g. internal security policy, Privacy Act
- Be easily findable:
- For paper-based terms, Farmers should be able to easily request a copy of the current terms from the Provider
- For digital terms, the terms should be available in several places e.g. on a product website before registration, at registration, and inside the platform once Farmer has agreed to them
- Be version controlled
- Address who has rights to control and use original, processed, and new data
- Clearly define the Provider's security and confidentiality responsibilities
- Be a fair and legal contract[1]. Some examples of unfair terms are:
- allow one party but not the other to avoid or limit performance of the contract;
- allow one party but not the other to terminate, renew or vary the contract; or
- exclude liability and/or provide broad indemnities.

Principle 1.2

Providers will:

Obtain clear, fully informed, and express consent from the Farmer as to the terms for collection, use, and sharing of Farm Data.

[1] https://www.fairtrading.nsw.gov.au/buying-products-and-services/guarantees,-contracts-and-warranties/contracts/unfair-contract-terms and https://jws.com.au/en/insights/articles/2021-articles/acl-unfair-contract-terms-vs-nsw-disclosure-obliga

Best practice for principle 1.2

- Silence, pre-ticked boxes, or inactivity, do not constitute consent
- Farmers should have to read the terms before agreeing to them, and understanding should be checked, e.g. in a digital setting this could be a few questions to test their knowledge
- Farmer should know what version of the terms they are agreeing to
- The agreed terms should have the date of agreement noted e.g. for electronic consent a date/time stamp should be recorded in the system
- Farmers should be able to obtain a copy of the agreed version of the terms
- Tracking consent against version of the terms is preferred (best practice). Alternatively, a date/time stamp of consent can be captured and compared to the version of the terms that was live at the time
- Reference from GDPR Recital 32 https://gdpr-info.eu/recitals/no-32/ :
  "EU GDPR(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

  This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.

  Silence, pre-ticked boxes or inactivity should not therefore constitute consent."

Principle 1.3

Providers will:

Provide prompt notice about any material changes to the terms and associated policies for collection, use, and sharing of Farm Data.

Best practice for principle 1.3

- Ideally Providers give at least 2 months' notice about material changes to terms
- Announcements of upcoming changes to terms should be communicated in several ways e.g. email, banner on product website and inside the digital product
- Material change is defined as a change that affects the intent of the agreement and/or rights or consequences to the parties. Trivial changes such as spelling and grammar, or changes to contact details, are not considered material (ref: Farm Data Code v2)
- Prompt notification can vary - e.g. in case of urgent changes to terms, only a week or a day may be able to be given. The outcome required is that notice is given to Farmers as early as possible. Prompt notice is required.

- Only providing a notification that terms have changed the next time that a user logs into the platform, is not enough, as some Farmers may not log into the platform for a long time.
- Also "reasonable endeavours" are not good enough for notification, notification has to be provided in some form.

Principle 1.4

Providers will:

Where a material change to terms and associated policies is proposed, obtain clear, fully informed, and express consent for the Farmer to accept the change and; provide an avenue for the Farmer to terminate the agreement without incurring a financial penalty and with adequate time to port or delete their Identifying Farm Data.

Best practice for principle 1.4

- Refer to best practice for obtaining express consent (see Best practice for Principle 1.2)
- Accepting or declining updated terms should be an easy process e.g. if electronic then clicking Accept or Decline, or being able to email the Provider with a simple sentence declining the changed terms
- Farmer should be given at least 2 months to port or delete their Identifying Farm Data before terms are changed

Principle 1.5

Providers will:

Provide a mechanism for Farmers to enquire about the collection, use, storage, security and sharing of Farm Data.

Best practice for principle 1.5

- Contact process should be easily findable by Farmers, e.g. clearly labelled on Provider's website, listed in the terms
- Data contact should be reachable by multiple channels during regular business hours (Mon-Fri 9am-5pm)
- Response times should be less than 3 business days

Principle 1.6

Providers will:

Notify Farmers of the legal jurisdiction in which Farm Data is stored or made available.

Best practice for principle 1.6

- This information should actively be provided to Farmers, e.g. listed in terms, or in an addendum
- Ideally Farm Data from Australian farms is stored, processed, backed up, and made available through Australian-based systems and networks only

Principle 2: Fairness

Fair and equitable use of Farm Data.

Principle 2.1

Providers will:

Ensure that Farmers get value from the use of Farm Data – including products and insights derived from it.

Best practice for principle 2.1

- There is a clear statement provided to Farmers on the benefits and value of sharing their Farm Data with the Provider, e.g. product improvements, discounts, reports or recommendations, getting Farm Data from up the supply chain

Principle 2.2

Providers will:

Ensure that Farm Data is not used to the detriment of Farmers without their clear, fully informed, and express consent.

Best practice for principle 2.2

Decisions about Farm Data collection, use, and sharing need to be evaluated for risk of detriment to Farmers. Some considerations include:

- Could Farmers be affected financially? e.g. affect market prices, land valuations, rent prices, equipment prices, contractor prices
- Could Farmers' reputations be affected?
- Could the health of Farmers, their families, their land, or their animals be affected?

If any of the answers are 'yes' then Farmers need to be notified and consent sought.

The Provider should also have a written Code of Ethics that covers Farm Data decisions, or it can be part of their Constitution to prioritise Farmer interest.

Principle 3: Control

Ability to control and access Farm Data.

Principle 3.1

Providers will:

Ensure the Farmer has control over who can access and use their Identifying Farm Data.

Best practice for principle 3.1

- Farmers should be able to nominate third parties of their choice to access their Identifying Farm Data, and through consent to the terms (and any changes to terms) Farmers can control whether their Farm Data is shared with third parties nominated by the Provider
- It is recommended that method for accessing Identifying Farm Data is electronic, and an audit trail is kept of all access events
- The identity and authorisation of any person accessing Identifying Farm Data should be validated
- OAuth2.0 is an example of best practice of users having to explicitly grant access for Provider A to share Farm Data with Provider B (and to have a pathway to revoke that access)
- There should be an easy way for authorised third parties to access Farm Data, e.g. API, or accessing Farm Data through a platform
- This principle does NOT require Farmers to be able to dictate to Providers which third parties of Provider's choice can and can't access Farm Data during the contract term – changes to third parties can only be made via changes to the terms

Principle 3.2

Providers will:

Take all reasonable steps to ensure any other entities permitted access to Farm Data are bound by the terms agreed between the Provider and Farmer, and do not contravene the provisions of this Code. This does not include entities nominated by the Farmer for data sharing purposes. Inform the Farmer where terms have not been fully passed on, or Code isn't complied with.

Best practice for principle 3.2

- Before granting access to Farm Data to a third party, the Provider should ensure that a contract exists and reflects the same terms around Farm Data management as those agreed with the Farmer
- Providers don't need to ensure that third parties are certified under the Code. It means that Providers need to communicate to third parties the Code principles with which they should be complying. Providers then accept responsibility and accountability under this Code if those third parties don't comply with the principles.

- This principle is relevant only for third parties who are permitted access to the data. Providers don't need to pass on terms to third parties that are providing hosting services only, if there are controls in place that prevent the hosting party from accessing the data e.g. data is encrypted in storage and hosting provider does not have the decryption keys.

Principle 3.3

Providers will:

Provide a mechanism for the Farmer to request corrections to Farm Data.

Best practice for principle 3.3

- Process should be easily findable by Farmers
- Process should be easy to action e.g. send an email to a support inbox
- Response times should be less than 1 month (aligns to GDPR)
- Providers don't necessarily have to make the requested corrections, but an explanation for why a change will not be made should be provided to the Farmer

Principle 3.4

Providers will:

Ensure Identifying Farm Data and any other data provided by the Farmer to the Provider, is not deleted without the Farmer's authorisation during any agreed or legally required data retention period.

Best practice for principle 3.4

- There should be a process for the Provider to ask a Farmer's authorisation before deleting their Farm Data
- Farmer should have a way of providing authorisation (consent) by way of physical or electronic means (see Best Practice for Principle 1.2)

Principle 3.5

Providers will:

Take all precautions to avoid identification or re-identification of a farm or Farmer from de-identified data, without the Farmer's clear, fully informed, and express consent.

Best practice for principle 3.5

- Providers first need to understand if they are working with Identifying Farm Data, e.g.:
- Datasets containing location data (e.g. address, GPS coordinates, region)
- Datasets containing other possibly identifying data such as animal or plant DNA data, soil data, spray data, the shape of the farm
- Identifying and Non-identifying Farm Data should be determined in consultation with Farmers where possible, as Farmers will understand their domain and can advise what data they are comfortable with being identifying
- The processes for de-identification and re-identification should be restricted to limited personnel and have segregation of duties so that no one person can re-identify the data. E.g. re-identification require at least two stages, each carried out by different people, and ideally approved by a third
- Identifiers should be stored in a separate database from the de-identified data, so that the data cannot be re-identified if one of the systems is breached
- Data can be de-identified and still remain useful: e.g. GPS coordinates can be de-identified by applying a positional shift or leaving the GPS data as is but standardising or normalising the data. This means that data is still mappable, but without knowledge of the true mean (and other statistical properties) and the type of transformation used, it is essentially de-identified.
- There should be a process for the Provider to ask Farmers' consent before re-identifying their de-identified Farm Data
- Farmer should have a way of providing consent by way of physical or electronic means (see Best Practice for Principle 1.2)

Principle 4: Portability

Ability to obtain and delete Farm Data.

Principle 4.1

During any agreed and legally required data retention period. Providers will:

Provide Farmers and/or their nominees with the ability to obtain all Identifying Farm Data (both raw and/or processed) in a structured and frequently used machine- or human-readable format where technically feasible.

Best practice for principle 4.1

- Farmers are entitled to obtain a copy of all Farm Data datasets that include their identifying information.
- Numeric/text data should be downloadable/exportable in common formats such as csv, txt
- Image data should be downloadable/exportable in common formats such as PDF, jpeg, png, where possible (some image data has specific file formats e.g. geospatial data)
- If being offered, database data should be provided in common database formats such as SQL (acknowledging that database structures can constitute IP for Providers and therefore are not expected to be shared)
- Where relevant, data should be interchanged using industry standard formats e.g. geospatial data GeoTIFF or GeoJSON
- Ideally, in addition to commo file formats such as csv, an API is also provided for easy porting of the data
- In case of a process where Farm Data needs to be requested from the Provider, turnaround times should be less than 1 month to action the request (aligns to GDPR)

Principle 4.2

During any agreed and legally required data retention period. Providers will:

Provide documentation to make ported data usable, e.g. Application Programming Interface (API) documentation and data model diagrams.

Best practice for principle 4.2

- Data models help to visualise relationships in data. Ideally a conceptual, a technical, and a physical data model should be provided with data, to make it easily understandable. It is acknowledged that some of this information might be the Provider's IP and not able to be readily shared without confidentiality agreements put in place first.
- Providing documentation such as data glossaries/dictionaries with definitions, formats, and logic rules, ensure the correct interpretation of the data is used, and therefore data integrity is maintained.

- API documentation should be provided with APIs, and give an example of every call, every parameter, and responses for each call. It should include code samples for commonly used languages such as Java, JavaScript, PHP, and Python. API documentation should provide an explanation for each API request and examples of error messages.

Principle 4.3

During any agreed and legally required data retention period. Providers will:

At the request of the Farmer, delete or dispose of any Identifying Farm Data, unless prohibited by law or unable to do so e.g. from a blockchain.

Best practice for principle 4.3

- Instructions on how to delete their Identifying Farm Data or request deletion, should be easy to find and action by Farmers (e.g. send an email to a support inbox, or use platform to delete data yourself)
- In case of a process where deletion needs to be requested from the Provider, turnaround times should be less than 1 month to action the deletion
- Confirmation of Farm Data deletion should be provided to the Farmer
- Deleting from backups: Principle 4.3 has no required time limit for deletion of the data, so as long as backups get over-written over time then that still meets the principle. There is no need to restore back-ups and delete data from them.
- Deleting from aggregated datasets: If data is Identifying Farm Data then farmers have the right to delete it even from an aggregated data set. If a Provider's model doesn't allow for this then they don't comply with the Code.
- Statutory retention requirements: Principle 4.3 has no required time limit for deletion of the data, so as long as it is eventually deleted that is ok.

Principle 4.4

During any agreed and legally required data retention period. Providers will:

Ensure that contingency plans exist to give Farmers the option to port and/or delete Identifying Farm Data in the event of insolvency.

Best practice for principle 4.4

- Farmers should be given immediate notice of insolvency, and clear instructions on how their Identifying Farm Data can be obtained and/or deleted

Principle 4.5

During any agreed and legally required data retention period. Providers will:

Provide the Farmer fair warning in advance of changes to legal jurisdiction, change of control, or sale of the Provider entity, and adequate time for the Farmer to port and/or delete their Identifying Farm Data.

Best practice for principle 4.5

- Farmer should be given at least 2 months' notice of such a change, and clear instructions on how their Identifying Farm Data can be obtained and/or deleted

Principe 5: Security

Keeping Farm Data protected and secure.

Principle 5.1

Providers will:

Take all reasonable and prudent steps, in line with industry best practice, to ensure Farm Data and any other data provided by the Farmer to the Provider, are protected at all times from unauthorised access, damage or destruction.

Best practice for principle 5.1

- Refer to sheet 'Security Controls' in the certification application form for a list of best practice security controls
- Implement forms of data transfer that are recognised as being not generally susceptible to third party interception or eavesdropping (e.g. end to end encryption)
- Global best practice for data security is to have a ISO27001 or equivalent information security management system that considers risks, defines policies and technical security procedures appropriate to the sensitivity of the data stored.
- Real Farm Data should not be used in test or demo environments
- Farm Data should be de-identified where possible (see Best Practice for Principle 3.5)

Principle 5.2

Providers will:

Put in specific data management protocols to protect sensitive data about the Farmer or farm, such as personal/financial information.

Best practice for principle 5.2

- There should be policies / processes in place to determine what is sensitive Farm Data
- Sensitive data should be determined in consultation with Farmers where possible, as they understand their domain and what data is especially sensitive and has serious consequences if breached
- Access to sensitive data should be restricted to only personnel that need to handle it in order to provide the product/service to Farmers
- Sensitive data should be de-identified where possible (see Best Practice for Principle 3.5)

Principle 5.3

Providers will:

Promptly notify the Farmer of a data breach that has led to unauthorised access to, or damaged or destroyed Farm Data.

Best practice for principle 5.3

- If a data breach occurs, then what should be communicated to impacted Farmers are the details of:
- What Farm Data was breached (e.g. date ranges, datasets)
- Who accessed it and when
- The extent of the data loss
- The mitigation plan for shutting down unauthorised access
- The recovery plan for retrieving and restoring Farm Data
- The prevention plan for preventing future breaches
- Regular updates on the progress of breach investigations and implementation of preventative controls should be provided to impacted Farmers

Principle 5.4

Providers will:

Implement a backup and recovery regime that is appropriate for the scale, sensitivity and timeliness of the Farm Data.

Best practice for principle 5.4

- Farm Data should be assessed in consultation with Farmers (where possible) for how critical it is to the running of farm operations (e.g. low, medium, high criticality)
- The back-up and recovery plan should address different levels of criticality (e.g. critical data needs more frequent back-ups and a quicker recovery)
- Ideally the most critical Farm Data would be backed-up at least every 24 hours
- Farm Data recovery times are ideally 1-3 business days for the most critical Farm Data
- Farm Data backups and archives should be handled with the same level of security as live data (e.g. encrypted, password protected, and physically secured)

Principle 5.5

Providers will:

Ensure all staff and sub-contractors that work with Farm Data, and/or set terms, policies, and/or processes for Farm Data are trained to comply with the terms of this Code.

Best practice for principle 5.5

- Mandatory training on Code principles and internal procedures relating to Farm Data management should be provided to new staff and sub-contractors that work with Farm Data, and repeated regularly to refresh knowledge
- Completion of training should be tracked per person
- The importance of the Code should be reinforced in relevant staff and sub-contractor communications
- New data management policies and procedures, and any changes to terms, should be checked against the Code to ensure they do not contravene the Code

Principle 6: Compliance

Compliance with disclosure obligations.

Principle 6.1

Where Providers are required by law to provide information to a third party, they will:

Avoid disclosing any Identifying Farm Data; or,

Best practice for principle 6.1

- In the first instance only de-identified Farm Data should be disclosed, and if that is not legally adequate only then should Identifying Farm Data be disclosed
- It is acknowledged that there could be circumstances where the Provider is legally obligated to disclose Identifying Farm Data, e.g. in the event of a fraud investigation. The Code does not seek to prevent a Provider from complying with any legal or regulatory obligations

Principle 6.2

If Identifying Farm Data must be disclosed, where legally permissible the Provider must promptly notify any Farmer whose information will be (or has been – if prior warning is not possible) disclosed.

Best practice for principle 6.2

- In the event of a legally required disclosure what should be communicated to Farmers is details of:
- What Identifying Farm Data needs to be, or has been, disclosed (e.g. date ranges, datasets)
- Whom it is being, or has been, disclosed to
- Purpose for which it is being, or has been, disclosed
- It is acknowledged that there could be circumstances where the Provider is legally prohibited from notifying the Farmer, e.g. in the event of a fraud investigation. The Code does not seek to prevent a Provider from complying with any legal or regulatory obligations

Best practice for specific use cases

Blockchain

A feature of blockchain is that data cannot be deleted from it.

Farmers need to be made aware of this when presented with terms for a blockchain based service, especially if Identifying Farm Data is going to be stored on the blockchain.

The permanence of data stored on the blockchain means careful consideration is needed about what data will be stored. For example, for traceability use cases it might be more appropriate for the region of origin for a beef product to be stored on the blockchain, rather than the name or location of the exact farm that produced it.

It is advisable not to store details that change frequently on the blockchain e.g. phone numbers, for risk that out of date data will be used/shared, unless of course there are accommodations for this in the solution design.

References

Title	Link	Comment
Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**) (Text with EEA relevance)	https://eur-lex.europa.eu/eli/reg/2016/679	GDPR legislation

Version history

Version	Version date	Author	Comments
0.1	12 July '22	Gabi Ceregra	Initial draft version, aligned to Data Code v1.5.1
0.2	13 July '22	Gabi Ceregra	Formatting and minor updates to draft version
0.3	8 Mar '23	Gabi Ceregra	Aligned to Data Code v1.6.2
0.4	16 Mar '23	Gabi Ceregra	Updated section on applying Code in scenario where there are multiple providers involved.
0.5	17 Apr '23	Gabi Ceregra	Aligned to Farm Data Code v2
0.6	24 May '23	Gabi Ceregra	Removed principle 6.1 (re Privacy Act obligations), and renumbered following principles
1.0	7 June '23	Gabi Ceregra	Final ready for publishing