Data Privacy and Use White Paper

Version 1.2 Updated: March 31, 2017

Table of Contents

DISCLAIMER

This document is for educational purposes only and does not purport to provide legal, financial, or other professional advice. This document is not all inclusive and is meant to provide broad guidance for the recipients of farm data and their customers. You should always consult your own attorneys and business advisors before finalizing a data privacy and use policy or agreeing to the terms of a data privacy and use policy.

Purpose of this White Paper

This white paper is a living document created to help educate the agriculture industry on incorporating data privacy best practices and standards into their operations. In addition, key terminology is included to encourage consistency across the industry.

It is also intended to provide recipients of Farm Data and their customers with areas to consider when using Farm Data. (For a definition of “Farm Data”, see the “Farm Data” section on page 5 of this document.) Samples of how Farm Data is used include:

- A farmer providing data to an agronomist or a service provider for the purpose of creating a variable rate planting prescription based on soil type and prior yearyield data.
- Equipment health and diagnostic data going directly from a tractor to an equipment manufacturer so that a dealer can alert the farmer about equipment issues or required maintenance.
- A service provider creating a work order to spray a pesticide within the boundaries of one or more grower fields.
- An agent of the grower providing summary planting information to the USDA.

The Role of AgGateway

The scope and range of available agriculture data is rapidly expanding. This data is being generated, collected, and managed in many forms across agriculture value-chain segments and the potential for this mass of data in its variety, velocity, and volume to impact agriculture is significant. AgGateway, as an industry eBusiness consortium, is in a unique position to help support the development of responsible data practices across the agriculture industry, including providing a source of information for ag stakeholders involved in the use and stewardship of Farm Data.

The role of Ag Gateway in Farm Data collection and use is to:

- Define common data categories or classifications.
- Develop standard and clear terminology for improving communication with farmers regarding privacy.
- Maintain a forum for the exchange of ideas surrounding data privacy and security best practices.
- Maintain collaborative relationships with industry stakeholders regarding proposed solutions to data privacy and security use and challenges.

Summary Concepts

Data privacy and use policies generally set out the ways that customer or client data is collected, used, disclosed, and managed. Policies may include consideration of the following concepts:

SECURITY & PRIVACY PROGRAMS

When defining security and privacy programs, consider whether the measures put in place are in line with industry best practices and are relevant to the organization and the data collected.

NOTICE, CHOICE, AND CONSENT

Consider providing parties with transparent choices (e.g., opt-in, opt-out) regarding use of their data as well as processes for stored data correction or removal.

NOTICE OF COLLECTION, USE, DISCLOSURE, AND SALE LIMITATIONS

Consider how transparency can be enhanced through clear descriptions of the collection, use, disclosure, and third party sharing of data. Consider providing contact information if warranted.

ACCOUNTABILITY

Evaluate how binding documents align across and support policies, privacy notices, contracts, and marketing materials.

Scope and Definition of Farm Data Management and Use

An unprecedented number of choices for integrated systems and solutions have driven the agriculture industry towards the use of data created by computers including but not limited to tractors, combines, environmental sensors, irrigation equipment, grain carts, and unmanned aerial systems. To facilitate the demand for these highly integrated systems and to reap the benefits while reducing risks, it is important to consider how data will be managed.

Farm Data has increasing value to farmers. At the same time, farmers are growing more aware of and sensitive to what this data may tell others about their operations. Farmers want transparency regarding the collection, use, sharing options and effective security controls for their data.

Farm Data

This list illustrates the broad scope of Farm Data and demonstrates the dynamic interaction of data between the farmer and the companies they works with to operate their business.

- Farm Management data
  - Business Operations
    - Financial & Tax
    - Operating & Land Loans
    - Office files
    - Capacity / Timing data
    - Farm Labor and Contracts
    - Human Resources
  - Supply Chain data
    - POS data
    - Partnerships
    - Customer data
    - Supplier data
  - Transport and Storage data
  - Commodity prices (input and output pricing)
  - Reporting and Compliance data

- Machine data
  - Rolling and Fixed Assets data
  - Energy & Fuel Use
  - Machine health and operation technique data
    - Machine Load
    - Equipment Reference data
    - Equipment Function

- Land data
  - Conservation data
  - Tillage practice data
  - Access data
  - Water management data
    - Source data
    - Usage data
  - Soil and fertility data
    - Soil Test data
    - Nutrient management data
    - Waste management data
  - Environmental and ecological data
    - Watershed data
    - Topological data
    - Elevation data and derivatives
    - Drainage data
  - Geospatial Information System (GIS), Global Positioning System (GPS), & Field Boundary data
    - Ground-based machine data
    - Unmanned Aerial System (UAS) data
    - Sensor Collection System (EC/EM) data
    - Remote sensing including Radar, Spectral, & Lidar data

- Agronomic data
  - Crop Seed data
    - Genetics data
    - Production Attribute data
  - Planting data
    - Recommendation data
    - Prescription data
    - Work Order data
    - As Planted data
  - Yield data
    - Attribute data
    - Quality data
  - Disease and Pest Management data
    - Crop Protection data (Herbicide, Insecticide, Fungicide)
    - Crop Protection Use and Application Rates data
    - Prescription data
    - Work Order data
    - As Treated / As Applied data
  - Crop Nutrition data
    - Sampling data
    - Application and use of Biological Fertilizer data
    - Application and use of Crop Protection Fertilizer data
    - Prescription data
    - Work Order data
    - As Treated / As Applied fertility treatment data
  - Pollinators

- Climate and weather data
  - Weather stations
  - Soil probes
  - Sensor data

- Livestock data
  - Breed
  - Genetics
  - Feed

- When combined with other data, Farm Data can be found in the following forms:
  - Raw Data
  - Processed Data
  - Anonymized Data
  - Aggregated Data
  - Derivative Data

Considerations regarding Farm Data Use[1]

When drafting policies, procedures, and agreements, the recipient of Farm Data should consider how it uses and distributes Farm Data. Customers should seek to understand how the Farm Data will be used and distributed when determining whether to enter into abusiness relationship with the prospective recipient.

AgGateway has developed the following questions for companies using Farm Data to consider as they establish policies, procedures, and agreements.

SECURITY & PRIVACY PROGRAMS

When defining security and privacy programs, consider whether the measures put in place are in line with industry best practices and are relevant to the organization and the collected data.

☐ Does your data agreement define a security program with applicable controls relevant to the data collected?

☐ Do your controls take into account when Farm Data combined with other data elements become PII (Personally Identifiable Information)?

☐ Can data be anonymous if it includes geospatial information? If so, what are the requirements and should farmers be made aware?

☐ What mechanisms should be put in place to effectively handle external stakeholder questions regarding the privacy and security of Farm Data?

NOTICE, CHOICE, AND CONSENT

Consider providing parties with transparent choices (e.g., opt-in, opt-out) regarding use of their data as well as processes for stored data correction or removal.

☐ Does the level of consent provided by the farmer match the intended use? For example, is access to and use of equipment diagnostic data limited to a farmer's equipment dealer if that was the only consent provided?

☐ What level of detail should be provided to farmers about the management of access and security controls protecting Farm Data?

☐ Should a farmer be allowed to have raw, aggregated, or anonymized data deleted?

☐ Should contractual agreements have a time restriction or limitation on use when a contract expires or is terminated?

☐ What constitutes full disclosure as to the intended use of the data in a binding agreement?

[1] This white paper does not define "owner" of Farm Data, as it is a legal term that is outside of the scope of this paper.

NOTICE OF COLLECTION, USE, DISCLOSURE, AND SALE LIMITATIONS

Consider how transparency can be enhanced through clear descriptions of the collection, use, disclosure, and third party sharing of data. Consider providing contact information if warranted.

- □ What data sharing options should be available to the farmer as it relates to Farm Data?
- □ Should data controlled by a farmer be shareable and transferable in an easily manageable form?
- □ Should companies inform farmers about the purposes for which they collect and use Farm Data?
- □ What level of detail is appropriate to provide farmers about the uses for which their Farm Data is collected?
- □ Should companies provide information about how farmers can contact the organization with inquiries or complaints?
- □ Should the contractual agreement specifically state entities or types of entities who get to access, view, analyze, delete, copy, export, and/or transfer data?
- □ Should limitations and conditions on the use and disclosure of Farm Data be clearly stated in contracts with farmers?
- □ Is a third party's use of Farm Data bound by the same limitations and conditions established in the original agreement between a farmer and a company? Is there a time limitation on the third party's use of the farmer's data?
- □ Should the data privacy and use policy guarantee that the recipients' other contracts and obligations comply with this policy?
- □ Should farmers be made aware that disclosure of Farm Data may be required through a subpoena or other court order?
- □ Should the contractual agreement specifically preclude use of the data to manipulate the market?
- □ Should a farmer receive value for the use of the Farm Data and other information derived from the Farm Data? Is the value what they may gain from better yields and lower input costs or is it compensation?

ACCOUNTABILITY

Evaluate how binding documents align across and support policies, privacy notices, contracts, and marketing materials.

- □ Who can authorize the use of Farm Data? Are there penalties for unauthorized use of Farm Data, and how is that determined?
- □ Do the agreements use standardized language in binding contractual agreements or clearly define terms as they are used?
- □ Should the data privacy and use policy provide for contractual damages for violations of the policy's terms and conditions?

Data Agreements

Data privacy and use policies generally reveal ways that customer or client data is collected, used, disclosed and managed by two or more parties.

Notices help to clarify expectations, understandings, and policies regarding Farm Data sharing between parties.

Data agreements are binding contracts between two or more parties. Things to consider when drafting data agreements:

- Transparency
- Policies, procedures, and agreements
- Third party sharing
- Definitions
- Security
- Applicable laws and regulations

Current Regulatory and Legal Requirements; Other Considerations

As is the case with all business operations, the development of an organization's data privacy and use policies and procedures necessitates that that legal and regulatory requirements are taken into account. Data privacy and use is an area of law that is constantly evolving and changing. For that reason and because this paper is intended to be educational in nature, this section contains only a sampling of laws, regulations, and practices that may be applicable as of the date of publication.

A full review of legal and regulatory considerations is not within the scope of this document. Companies are encouraged to engage legal counsel to identify applicable laws and regulations when creating their data privacy and use policies.

SAMPLING OF LAWS AND REGULATIONS

Personally Identifiable Information (PII)

Companies that store or manage Personally Identifiable Information (PII) may be legally obligated to protect this data. The definition of PII may vary among various federal and state regulations. Companies should engage legal counsel to review the data being collected and stored to determine which PII laws and regulations apply, if any.

One of several definitions of PII is as follows:

> PII, as used in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context…. NIST Special Publication 800-122 defines PII as "any information about an individual maintained by an agency including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[2]

Additionally, under the Risk Management Agency (RMA) of the United States Department of Agriculture (USDA), PII encompasses "Protected Information," which is any PII about a crop insurance policyholder, or information about the policyholder's farming operation or insurance policy, acquired from the policyholder, USDA, the Comprehensive Information Management System, or the policyholder's previous or current approved insurance provider or agent that is protected from disclosure by the Privacy Act of 1974 (5 U.S.C. § 552a), section 502(c) of the Act (7 U.S.C. § 1502(c)), or any other applicable Federal statute. This definition includes all hard copy or electronic information.[3]

Some online resources that may be helpful in understanding PII are:[4]

- The National Institute of Standards and Technology, U.S. Department of Commerce Special Publication 800-122, Guide to protecting the confidentiality of Personally Identifiable Information (PII).[5]
- United States Department of Labor, Guidance On The Protection Of Personal Identifiable Information.[6]
- U.S. Department of Commerce Office of the Chief Information Officer, Department of Commerce IT Privacy Policy.[7]
- The International Association of Privacy Professionals (IAPP) provides a downloadable Global PII Directory spreadsheet that catalogs definitions of PII under various international, federal, and state laws.[8]

[2] Personally identifiable information. (n.d.). Retrieved November 1, 2014, from http://en.wikipedia.org/wiki/Personally_identifiable_information

[3] USA, Risk Management Association, Federal Crop Insurance Corporation. (2014, July 1). Standard Reinsurance Agreement. Retrieved fromhttp://www.rma.usda.gov/pubs/ra/sraarchives/15sra.pdf

[4] AgGateway cannot confirm the validity or accuracy of the information on these websites. They are listed for information only.

[5] Mccallister, E., Grance, T., & Scarfone, K. A. (2010). Guide to protecting the confidentiality of Personally Identifiable Information (PII). doi:10.6028/nist.sp.800-122

[6] Guidance on the Protection of Personal Identifiable Information. (n.d.). Retrieved February 2, 2016, from http://www.dol.gov/general/ppii

[7] IT Privacy. (n.d.). Retrieved February 2, 2016, from http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/index.htm

[8] International Association of Privacy Professionals. (n.d.). Global PII Directory. Retrieved February 2, 2016, from https://iapp.org/resources/article/global-pii-directory

Freedom of Information Act Considerations (FOIA)

Private parties that collect and manage Farm Data are not generally subject to FOIA. FOIA applies to Executive Branch departments; agencies and offices; federal regulatory agencies; federal corporations; and government contractors keeping records for the federal government. Congress, the federal courts, and parts of the Executive Office of the President that function solely to advise and assist the President, are not subject to FOIA. Records obtainable under FOIA include all "agency records" such as print documents, photographs, videos, maps, e-mail, and electronic records that were created or obtained by a federal agency and are, at the time the request is filed, in that agency's possession and control.[9] Companies that manage and share Farm Data with governmental entities to which FOIA applies should be aware that the shared data is most likely subject to FOIA.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.[10] Any data and privacy policy should comply with the Gramm-Leach-Bliley Act if the company is subject to the Act.

Insurance Considerations

Every insurance company issuing a data collection or use agreement is obligated to ensure that the agreement is aligned with applicable insurance law. The National Association of Insurance Commissioners (NAIC) provides resources, such as compendia of state law, which can assist in determining the applicable laws in your state.[11] Insurance company data and privacy policies should comply with applicable state insurance laws.

Harmonizing data usage obligations between non-binding documents and binding agreements

When creating privacy policies, guiding principles, and data usage agreements consider supporting and harmonizing them in related legal agreements.

Data RetentionConsiderations

Most companies adopt formal data retention policies for effective data management. Consideration of legal data retention requirements is important when formulating these policies and procedures.

[9] National Security Archive, George Washington University. (n.d.). FOIA Basics. Retrieved February 2, 2016, from http://www2.gwu.edu/~nsarchiv/nsa/foia/guide.html

[10] Gramm-Leach-Bliley Act. (n.d.). Retrieved February 2, 2016, from https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

[11] National Association of Insurance Commissioners (NAIC). (n.d.). Map of NAIC States & Jurisdictions. Retrieved February 2, 2016, from http://www.naic.org/state_web_map.htm

Appendix A: Terminology

Terms included in Ag Glossary

AgGateway has introduced a comprehensive agricultural glossary that can be freely accessed and used by the industry to facilitate accurate communications. The glossary is an online wiki for agriculture terms, definitions, acronyms, key words and synonyms. The glossary pulls from a number of established industry and government sources.

The following terms have been submitted to the Ag Glossary by the AgGateway Data Privacy and Security Committee:

Ag Tech Provider - A business or service that furnishes and supports agricultural technology, engineering, and applied sciences to farmers and farm operations.

Aggregated data - Factual information that has been digitally encoded and formed by the collection, conjunction or compilation of data into a whole mass or sum; it is the sum, mass, or assemblage of data. Data is information that is converted into a binary digital form for the purpose ofcomputing.

Big Data - Big data is high-volume, high-velocity and high-variety information assets that demand cost- effective, innovative forms of information processing for enhanced insight and decisionmaking.

Data - A general term to denote factual information. Data is information that is converted into a binary digital form for the purpose of computing. It is digitally encoded information.

Data Anonymization : Technology that converts clear text data into a nonhuman readable and irreversible form, includingbut not limited to preimage resistant hashes (e.g., one-way hashes) and encryption techniques in which the decryption key has been discarded. Data anonymization enables the transfer of information across a boundary, such as between two departments within an agency or between two agencies, while reducing the risk of unintended disclosure, and in certain environments in a manner that enables evaluation and analytics post-anonymization.

Data (Network Communications) — Information that identifies the main content of a transmission unit as distinguished from “control information,” “control bits,” and/or other similar terms.

Data (Telecommunications) — Digitally encoded information (data) that can be transmitted with intermittent connections in packets (as distinguished from analog-encoded information, such as a conventional telephone voice call) that requires a dedicated, continual connection for the duration of transmissions.

Data Access Management – The activity to manage the access to and the use of data.

Data Buckets — Specific data element(s) used to categorize / filter data within a database field that can be used to sort and filter data within the field and required to execute an operation or process.

Data Collection — The systematic gathering and measuring of data that ensures the accuracy of the information collected and enables the analysis and interpretation of that information.

Data Communication — The electronic transmission and exchange of data between a source that transmits data and a receiver that receives data.

Data Consumer – A person, group, or organization who is the user of data collected and/or analyzed. The data is not changed, improved or devalued by the use of theconsumer.

Data Dictionary – A data dictionary is a database that contains data definitions and database structures. It serves as a catalog of all data elements, containing their names, structures, and information about their usage, for the benefit of programmers and others interested in the data elements and their usage.

Data Dictionary Identifier —An ID that uniquely and permanently identifies an object and/or parameter within a data set; i.e. (in a ISO 11783-11 data dictionary).

Data Element – A data element is a generic term that identifies an atomic (smallest) unit of data that has precise meaning or precise semantics. It consists of group of characters that specify: 1) an identification, 2) representative terms, 3) enumerated value or code, and 4) a list of synonyms; at the basic level it is a qualifier, value, or text that can be registered. It is a basic unit of information built on standard structures having a unique meaning and is one separate item (smallest piece) of information that has a unique meaning, which may be made up of combination of characters or bytes that has distinct units or values.

Data Governance – There are two functional definitions:

1) Data Governance: The activity to ensure data definitions are clear and concise, do not overlap with other data definitions and meet the requirements for the domain they are defined for.
2) Data Use Governance, a synonym of data access management.

Data Privacy – Data privacy is the assurance that a person's or organizations personally identifiable information is not inappropriately disclosed. Ensuring data privacy requires data access management, eSecurity, and other data protection efforts.

Data Processing — Any method or technique, including automated and repetitive activities, to collect, store, classify, retrieve and manipulate data to produce information sets.

Data Protection —Data protection identifies the security of data storage and protection of the data collected to be used only for the purpose for which it is collected. Data protection standards include: data collected cannot be disclosed to other parties without the consent of the party owning or submitting (via permission of the owner) the data; any data shared must protect any personally identifiable information; the data cannot be sent to any other location without the consent of the party owning or submitting (via permission of the owner) the data; and the receiving party must have secure data protection storage and processes to handle the data.

- Data protection is the responsibility of the party collecting data from another party for the purpose of using that data for a business reason; the party submitting the data has the right and obligation to correct any factually incorrect datasubmitted.

- Continuous Data Protection (CDP) - An approach to recovery that continuously, or nearly continuously, captures and transmits changes to files or blocks of data while journaling these changes. This capability provides the option to recover many more-granular points in time to minimize data loss, and enables arbitrary recovery points. Some CDP solutions can be configured to either capture data continuously (true CDP) or at scheduled times (nearCDP).

- Data Loss Protection (DLP) - Data loss protection describes a set of technologies and inspection techniques used to classify information content contained within an object — such as a file, email, packet, application or data store — while at rest (in storage), in use (during an operation) or in transit (across a network). DLP tools also have the ability to dynamically apply a policy — such as log, report, classify, relocate, tag and encrypt — and/or apply enterprise data rights management protections.

Data Scale — Term associated with Big Data used to determine the magnitude of the database set. The larger the data scale, the greater the number of information pieces included in the set, leading to enhanced analysis of the data within the set.

Data Security – The protection of data and a database from destructive forces, internal and external, and unwanted actions of unauthorized users. Data security involves but is not limited to data encryption, file backup, data masking, and disk encryption.

Data Stakeholder — An individual or group that has an interest or concern in the operation, or organization, where the data originated or is managed and/or have a perceived benefit from access or analysis of the data; those who use, affect, or are affected by data.

Data Standards — The agreement of multiple, various organizations and/or standards organizations on common data definitions, data representation, data use and usage, data management, and data structures to which all data layers must conform that ensures parties sharing or exchanging information have a common understanding of what the information represents and how it is communicated.

Data Steward — A data steward is an expert (person or organization) who manages and maintains another's data or information to ensure that the data or information can be used to draw conclusions or make decisions. Data stewards are responsible for data quality; they are responsible for serving and protecting the data owner's/data consumer's needs, assets, and data integrity.

Data Stewardship — The management and care of one's own or another individual's or organization's data assets to ensure the accessibility, security, and integrity of those dataassets.

Data User (Usage) – See Data Consumer

Decision Rights - A system developed and utilized to determine who makes a decision — and when, how, and under what circumstances the decision is made. Formalizing decision rights is a key function of data governance.

Decision Support System - The term originally described computer system designed to collect, store, process, and provide access to information to support managerial decision making.

Derivative Data - Data generated from analysis of other datasets.

eBusiness: The application of electronic information and communication technologies in support of all the activities of business; it is any activity of business that is conducted using electronic media, information or communication technology.

eSecurity: The application of practices, technology, and systems to protect and defend electronic information and communication technologies from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Farm Data - A specific term to denote factual agricultural information created, generated, transmitted, or used in a farming operation. It is agricultural information that has been converted into a binary digital form for the purpose of computing.

Farmer - A person engaged in agriculture, raising living organisms for food or raw materials; a person who operates a farm or cultivates land. The term applies to individuals who do some combination of raising field crops, orchards, vineyards, poultry, or other livestock. A farmer might own the farmed land or might work as a laborer on land owned by others.

Information security: The practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc...); it is sometimes shortened to InfoSec.

Information Technology (IT) security: Information Technology security is information security applied to technology (most often some form of computer system). A computer is any device with a processor and some memory (even a calculator). IT security is responsible for keeping all of the technology within the company secure from malicious cyber-attacks and/or unauthorized use that attempts to breach into critical private information or gain control of the internal systems. IT security is sometimes referred to as computer security.

Information assurance: The act of ensuring that data is not lost when critical issues arise. These issues include but are not limited to: natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issuesoccurs.

Operator - The farm operator is the recognized operator overseeing the farm operation. The operator may or may not be the primary operator of the ag machinery. Other names are: client, grower, farmer, and producer.

Processed Data - Farm Data that has been prepared or modified by a systematic series of actions or processes to achieve a projected end or use.

Producer - A person engaged in producing an agricultural commodity for a share of the insured crop, or the proceeds thereof; the entity that is the recognized legal operator of the farm operation. The producer may or may not be the primary operator of the ag machinery, but is the primary decision maker in the agronomy and other crop husbandry decisions. Other names are- client, farmer, andoperator.

Raw Data - See Data.

Third party - Any additional party to an incident between two parties; an additional party involved in a transaction between two parties; examples - business, affiliate, provider, advisor, cooperative, custom service operator, etc.

Wireless Data Communication - Wireless Data Communication is a form of communication that uses the radio spectrum rather than a physical medium. It may carry analog or digital signals and may be used on LANs or WANs in one- or two-way networks.

Other terminology resources

The Data Governance Institute (DGI) provides an online glossary of terms used in data governance and data-related disciplines, such as data privacy and compliance. http://www.datagovernance.com/glossary-governance/

The International Association of Privacy Professionals (IAPP) provides an online Glossary of Privacy Terms. https://iapp.org/resources/glossary

APPENDIX B: Policies and statements related to data and privacy in agriculture

Ag industry groups and agriculture companies have published their own statements of principles and policies related to data privacy in agriculture.

Because these policies and statements are frequently updated, links to independent organizations' data privacy principles and policies can be found on the AgGateway Data Privacy and Security Committee page Examples: Data Privacy Principles and Policies in Agriculture.

The list is intended to provide a range of examples; it is not meant to be a complete list. If you are aware of a privacy policy or statement the Committee should add to the list or you notice an outdated link, email the Data Privacy and Security Committee leadership noted on the Committee homepage.