# Table of Contents

Purpose of this Whitepaper .................................................. 3  
The Role of AgGateway ....................................................... 3  
Farm Data ............................................................................. 4  
Control of Farm Data .......................................................... 5  
Scope and Definition of Farm Data Management and Use .......................................................... 6  
  Current Legal Requirements .................................................. 6  
  Considerations Regarding Farm Data Use, Control & Ownership .................................................. 7  
Key Communications / Documentation ...................................... 10  
  Data Agreements .................................................................. 10  
  Farm Data Policies ............................................................... 11  
Appendix A: Terminology ....................................................... 12  
  Resources ............................................................................ 16  
Appendix B: Industry Groups Policy Statements on Big Data / Data Privacy ..................................... 17  
  American Farm Bureau Federation ...................................... 17  
  American Soybean Association ............................................ 18  
  National Corn Growers Association ..................................... 18  
  National Farmers Union Policy ............................................ 19  
APPENDIX C: Grower Information Services Cooperative Privacy Policy ........................................... 20  
APPENDIX D: Ag Companies Policies on Big Data / Data Privacy ...................................................... 22  
  CNH Industrial .................................................................... 23  
  Climate Corporation ............................................................. 25  
  John Deere .......................................................................... 33  
  Monsanto ............................................................................ 37  
  Raven Industries ................................................................. 51
Purpose of this Whitepaper

This Whitepaper is a living document and has been created to identify key terminology and a framework the agriculture industry can use to consider how to establish the data privacy and use standards, practices, and procedures for their farm customer or business operation. These data privacy concepts should be considered when developing a data privacy and security policy and/or program(s) to include Farm Data.

The Role of AgGateway

The scope and range of data available pertaining to agriculture is rapidly expanding. This data is being generated, collected, and managed in many forms throughout the value-chain segments within agriculture. The potential for this mass of data in its variety, velocity, volume to impact agriculture is significant. AgGateway, as an industry eBusiness consortium, is in a unique position to identify, clarify, and standardize terminology affecting the various practices involved in collecting, sharing, using, analyzing and disseminating such information to and from interdependent systems. AgGateway provides the industry a forum for raising awareness of the community of Ag stakeholders involved in the use and stewardship of this rapidly expanding Farm Data frontier.

The role of Ag Gateway surrounding Farm Data use, analysis and transfer is to:

▲ Define how data should be categorized and/or classified in Ag (e.g., personally identifiable information, insurance and financial data, farm data).

▲ Develop standardized and clear terminology to help stakeholders understand and communicate the conditions for creating, sharing and transferring Farm Data.

▲ Identify and reference actions on standards involving Farm Data use and sharing.

▲ Maintain a forum for the exchange of ideas surrounding the best practices for the security and privacy of Farm Data stakeholders.

▲ Maintain collaborative relationships with industry stakeholders regarding proposed solutions.
Farm Data

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

▲ Farm Operations & Management data
  o Financial
  o Tax
  o Office files
  o Capacity / Timing data
  o Farm Labor and Contracts
  o Human Resources

▲ Supply Chain data (e.g., partnerships, customer & supplier information)

▲ Rolling and Fixed Assets data

▲ Machine health and operation technique data
  o Equipment Reference data
  o Fuel Usage data
  o Equipment Function

▲ Land data
  o Watershed data
  o Drainage data
  o Conservation data
  o Tillage practice data
  o Access data

▲ GIS, GPS and Field Boundary data
  o Ground-based machine data
  o Unmanned Aerial System (UAS) data
  o Sensor Collection System (EC/EM) data
  o Radar, Spector, Lidar data
  o Imagery data

▲ Crop Seed data
  o Genetics data
  o Production Attribute data

▲ Planting data
  o Recommendation data
  o Prescription data
  o Work Order data

▲ Energy Use

▲ Water management data
  o Source data
  o Usage data

▲ Disease and Pest Management data
  o Crop Protection data (Herbicide, Insecticide, Fungicide)
  o Crop Protection Use and Application Rates data

▲ Biological data
  o Crop Nutrition data
    o Sampling data
    o Application and use of Biological Fertilizer data
    o Application and use of Crop Protection Fertilizer data

▲ Pollinators

▲ Yield data
  o Attribute data
  o Quality data

▲ Soil and fertility data
  o Soil Test data
  o Nutrient management data
  o Waste management data

▲ Environmental and ecological data
The data listed below are likely governed by bodies of law in the United States:

- Protected Personal Information (PII)
- Protected Health Information (PHI)
- Insurance information
- Financial information
- Equity and real estate data

The Farm Data when combined with other data can be found in the following forms:

- Raw Data
- Processed Data
- Anonymized Data
- Aggregated Data
- Derivative Data

### Control of Farm Data

Some issues to be addressed when defining control of Farm Data are:

1. Identifying who can authorize Farm Data use
2. Establishing proper access controls ensuring appropriate level of access for who gets to view and/or use the Farm Data
3. Establishing standardized protocols for securely transferring Farm Data and developing transfer and retention policies (e.g., who transfers what to whom and how)
4. Identifying limitations of data transfers that allows the farmer to determine who can do what with what Farm Data
Scope and Definition of Farm Data Management and Use

Numerous forces have driven the agricultural 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 this advancement and reap its benefits while reducing the risks, it is important to consider how data is managed and used together with the potential benefits to agricultural production.

Today’s farming architecture brings to bear the power of technological innovation. From the planters to combines the farmer has at his or her fingertips real-time data that when analyzed and integrated in their farming processes will optimize their farming operations. These analyzed data elements provide key insight into the farming operation, the farmer's financial position, and its future potential in the Industry.

Farm Data has increasing value to the farmer. They are growing more aware and sensitive to what this data tells about their operations. Because of this, farmers want transparency regarding the purpose of use for their data; who it is shared with and have a choice in authorizing these activities.

CURRENT LEGAL REQUIREMENTS

COMPLIANCE WITH LAWS AND REGULATIONS

Any data collection and use agreements shall comply with applicable laws and regulations. They include, but are not limited to:

Personally Identifiable Information (PII)

Every company which stores or manages Personally Identifiable Information (PII) is obligated to protect this data and comply with applicable data protection laws.

Personally Identifiable Information (PII) 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. PII is 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, employment information, and field Geographic Information System (GIS) boundary information.

Freedom of Information Act Considerations

Private parties that collect and manage Farm Data are not subject to the FOIA. However, if a government entity or government contractor somehow obtains possession of the data controlled by the farmer, that data may become subject to the FOIA. In addition, a subpoena or other court order could require private companies to produce Farm Data to a court or to other parties, including the government.
The FOIA applies to Executive Branch departments, agencies and offices; federal regulatory agencies; and federal corporations. 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 the FOIA. Records obtainable under the 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.¹

Financial Considerations

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.²

Insurance Considerations

Every company which issues a data collection and use agreements is obligated to assure that the agreement is aligned with applicable insurance law. Here is a reference: http://www.naic.org/state_web_map.htm

Data usage obligations shall be harmonized between non-binding documents and binding agreements

Privacy Policies, Guiding Principles, and Data Usage Agreements should be supported by a company’s legal agreements.

CONSIDERATIONS REGARDING FARM DATA USE, CONTROL & OWNERSHIP

DISCLAIMERS

▲ Farm Data ownership is not a principle or definition that AgGateway will address. It is the responsibility of each company to determine their policy on this issue. As companies review data ownership they should consider the following:
   o Is it the farmer or the landowner who controls Farm Data? Or someone else? Or some combination of people or entities?
   o Who controls application data, is it the cooperative or service provider who applies the herbicides or the farmer who pays for the application? Or the landowner?
   o Who controls harvested production data, is it the owner of the combine or the owner of the crop which it harvested?
   o Under a crop/share agreement, does the landowner or the farmer control the Farm Data?

¹ Notes taken from The George Washington University National Security Archive: http://www2.gwu.edu/~nsarchiv/nsa/foia/guide.html
² Bureau of Consumer Protection Business Center
If a landowner is being required to prove compliance with an environmental regulation, can he or she do so if the farmer controls the Farm Data?

If the landowner controls the Farm Data, does it lead to higher rental rates for the tenant?

For purposes of this paper, the term “Farm Data” includes “data” or “raw data”. The committee will review and update these definitions as work progresses.

For purposes of this paper, the term “third party” includes various terms such as partner, business partner, affiliate, third party, etc. The committee will review and update these definitions as work progresses.

For purposes of this paper, AgGateway took the position that the farmer controls the usage of his or her Farm Data.

For purposes of this paper, AgGateway focused on what should be considered when developing policy for control of certain agreements with farmers.

CONTROL OF FARM DATA

AgGateway has developed the following questions for each company using Farm Data to consider as they establish their policies and agreements regarding Farm Data. Since we are not addressing ownership, we have centered the considerations on who controls the data.

Should Farm Data be collected by systems hosted by an Ag Technology Provider (ATP) only with the affirmative consent of the farmer?

Should a farmer have the ability to control any form of Farm Data concerning his or her farm or farming practices, including data collected by technology equipment?

Should a farmer be able to contractually limit the use, sale and disclosure of his or her Farm Data now and in the future?

Should farmers have multiple participation options for data sharing in each of their relationships with ATP’s?

Should ATP’s use standardized language in binding contractual agreements?

Any data collection and use agreements should clearly identify data privacy and security policies and or practices. Following are a series of questions that should be considered:

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

Does your data collection and use agreement reference any relevant data privacy and security laws and policies?

Do your agreements clearly define terms as they are used?
Does your data collection and use agreement ensure the security of the data controlled by the farmer?

Does your data collection and use agreement identify what the farmer’s responsibility is in supporting the ATP in security of the data?

OTHER DATA AGREEMENTS

Any data collection and use agreement should clearly identify data control policies or standards. Following are a series of questions that should be considered by Ag Technology Providers (ATPs):

▲ Should the ATP ensure that limitations and conditions on the use and disclosure of Farm Data are clearly stated in contracts with farmers?
▲ Should ATPs be required to inform farmers about the purposes for which they collect and use Farm Data?
▲ Should ATPs provide information about how farmers can contact the organization with any inquiries or complaint?
▲ Should the ATP contractual agreement specifically state who gets to access, view, analyze, delete, copy, export, and transfer data?
▲ Should the ATP contractual agreement specifically state for what purposes the Farm Data may be used?
▲ What constitutes full disclosure from an ATP as to the intended use of the data in a binding contract?
▲ Should the ATP contractual agreement have a time restriction on use?
▲ Can the ATP contractual agreement assure the farmer that none of the data that is transferred to an ATP can be made public via a Freedom of Information Act (FOIA) request?

OTHER ISSUES

▲ Should individuals and ATPs that create, maintain, use or disseminate data be accountable for ensuring non-binding and binding agreements are consistent with the defined policies?
▲ Should ATP agreements addressing Farm Data include; (a) security; (b) individual choice and consent; (c) collection, use, disclosure and sale limitation; (d) data quality and integrity; (e) accountability; and (f) guidelines for remuneration?
▲ Should we need to educate farmers about the reality of what is and isn't in the terms of conditions and other legal contracts?
▲ How should farmers be made aware that disclosure of Farm Data may be required through a subpoena or other court order?
▲ Can data be anonymous if it includes the geospatial info? If so, what are the requirements and should farmers be made aware?
▲ Should data controlled by a farmer be shareable and transferable in an easily manageable form?
▲ Should a farmer be allowed to have aggregated or anonymized data deleted?
▲ How long should Farm Data be retained by the ATP? Should a farmer be made aware of this timeline and what the disposition of the data is once removed?
▲ Is a third party’s agreement bound by the same limitations and conditions established in the farmer/ATP original contract?
▲ 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 generated from the Farm Data? Is the value what they may gain from better yields and lower input costs or is it compensation?
▲ Is Farm Data different than a farmer produced commodity? Should a farmer be paid for access to the Farm Data under the farmer’s control?

**Key Communications / Documentation**

It is important to clarify expectations, understandings, and policies regarding Farm Data between the farmer and the company he/she is working with. Communication and documentation that is clear, concise, and complete is necessary and should be a part of data collection and use agreements.

**DATA AGREEMENTS**

All data agreements created by a company and issued to a farmer:

- Shall comply with applicable laws and regulations.
- Shall be harmonized between non-binding documents and binding agreements.
- Shall reference any relevant data privacy and security policies.
- Should address any current or future third-party interests regarding data privacy and security obligations.
- Should use standardized entity definitions such as third party, affiliate, business partner, etc.
- Shall define a Security Program, which will be based on controls relevant to each organization.
FARM DATA POLICIES

Entities engaged in the practices outlined in this paper should develop or adopt a policy suitable for their specific enterprise. Such policies should consider, but not be limited to the following:

A. POLICIES/SECURITY/SAFEGUARDS

Security Program Defined – Consisting of Industry best practices and based on controls relevant to the parties to the agreement.

B. INDIVIDUAL CHOICE AND CONSENT ON HOW FARM DATA IS USED

Choice and Consent: the act or instance of selecting from a number of possibilities; the right, power, or opportunity to choose (pick by preference).

Organizations should give farmers the opportunity to choose (opt out) whether their Farm Data will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual.

C. COLLECTION, USE, DISCLOSURE, SALE LIMITATION

Organizations shall notify farmers about the purposes for which they collect and use Farm Data. They must provide information about how farmers can contact the organization with any inquiries or complaints, the types of third parties to which they disclose the Farm Data and the choices and means the organization offers for limiting its use and disclosure.

Data Access: Farmers should have access the Farm Data and be able to delete or correct and amend where it is inaccurate.

D. ACCOUNTABILITY

Accountable: Individuals and organizations creating, maintaining, using or disseminating data must be accountable for ensuring non-binding and binding agreements are consistent with the defined policies. Applicable policies shall be made available to the parties upon request (if not published.).
Appendix A: Terminology

This appendix is a list of industry terms and definitions as defined by the AgGateway Glossary Working Group and to be modified by the 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 of computing.

**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 decision making.

**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, including but 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 the consumer.
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 data submitted.

- 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 (near CDP).
- **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 data assets.

**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 issues occurs.

**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, and operator.
**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.

**RESOURCES**

http://www.datagovernance.com/glossary-governance.html

http://ori.dhhs.gov/education/products/n_illinois_u/dfront.html
Appendix B: Industry Groups Policy Statements on Big Data / Data Privacy

This information reflects the publicly available big data / data privacy policies for farm groups.

AMERICAN FARM BUREAU FEDERATION


Proprietary data collected from farming and agricultural operations is valuable, should remain the property of the farmer, and warrants protection.

We support:

--Efforts to better educate farmers and ranchers regarding new technology or equipment that may receive, record, and/or transmit their farming and production data;

--Requiring companies that are collecting, storing, and analyzing proprietary data to provide full disclosure of their intended use of the data;

--Formation of standardized protocols regarding privacy and terms of conditions to ensure a standard definition of all components within the contract. Farm Bureau should be an active participant in developing these protocols;

--Compensation to farmers whose proprietary data is shared with third parties that offer products, services or analyses benefitting from that data;

--Multiple participation options being included in all contracts;

--All proprietary information between the farmer and the company remaining between the two entities. This would not preclude a farmer from sharing data with whomever he/she chooses (for example, a consultant);

--Utilizing all safeguards to ensure proprietary data is stored at an entity that is not subject to a Freedom of Information Act (FOIA) request;

--The farmer’s right to enter into agreement and their rights to sell their proprietary data to another producer (for example in a land sale);

--Private companies entering into agreements which would allow for the compatibility/updating of equipment and updating of software; and

--The right of a farmer to have access to their own data, regardless of when it was shared with a company.
--The right of a producer who no longer wishes to participate in aggregated data sharing with a private company, to remove their past aggregated data from the company’s database and revoke that company’s ability to sell or use that data in the future.

We oppose any federal agency or FOIA-eligible entity from serving as a data clearing house for all proprietary data or aggregated data collected by private companies.

AMERICAN SOYBEAN ASSOCIATION

http://soygrowers.com/

ASA realizes that production data such as field maps, soil tests, production records, images and input records have monetary value. ASA believes this information gathered by GPS, GIS, or other precision farming practices remain the sole property of the owner and/or operator, or their agent, based on their respective investment, regardless if the data collection was voluntary or involuntary. This information should not be used, released or sold without consent.

ASA supports national agricultural organizations working together on behalf of farmers and with industry to develop industry and data standards to clarify policy for the acquisition, ownership, valuation and utilization of Farm Data and to provide educational opportunities for farmers on best use practices.

ASA opposes any entity from serving as a data clearinghouse for all proprietary data without prior written farmer consent from the farmer who owns the data.

NATIONAL CORN GROWERS ASSOCIATION

http://www.ncga.com/home

Information gathered by precision farming practices should remain the sole property of the farm operator excluding any other contractual arrangement. This information should not be used, released, or sold without their consent.

We believe that data collected from farming and agricultural operations is valuable, should remain the property of the individual, and warrants protection.

We will:

--Support efforts to better educate stakeholders regarding utilizing new technology or equipment that may receive, record, and/or transmit their data.

--Support requiring companies that are collecting, storing, and analyzing the data to provide full disclosure of their intended use of the data.
--Seek formation of and be an active participant in industry discussions regarding development of industry wide protocols including, but not limited to, proper disclosure, privacy, and use agreement.

--Encourage participants in data sharing use agreements to recognize the value associated with the data; allowing farmers to receive fair compensation.

--Encourage designers of precision farming equipment to use communication standards to make their products compatible with other brands of software and hardware.

**NATIONAL FARMERS UNION POLICY**

[http://www.nfu.org/privacy-policy](http://www.nfu.org/privacy-policy)

Detailed field data should only be collected with the producer’s consent in a manner so as to:

1) Ensure data collected remains the property of the producer;

2) Protect privacy;

3) Avoid consolidation of market power;

4) Maintain competition; and

5) Prevent manipulating markets.
APPENDIX C: Grower Information Services Cooperative Privacy Policy

www.gisc.coop

GIsc’s Value Proposition – Key Points

http://www.gisc.coop/about-gisc/giscs-value-proposition/

1. GiSC realizes that during the production of commodities the process “spins” off vast amounts of information that is valuable to the Grower and others in the marketplace.
2. GiSC believes that the future of efficient information flow must involve a system that assists in the collection, storage, access, and sharing of the Grower’s information, but the access to that information must TOTALLY be under the Grower’s control.
3. GiSC believes that the Grower must CONTROL the operation’s information, but that CONTROL is not enough.
4. GiSC believes that the Grower must OWN the operation’s information. GiSC will fight for the Grower to CLAIM ownership rights in all data that originates from the farm.

Growers’ Bill of Digital Rights


1. U.S. Agriculture Producers have the RIGHT TO CLAIM OWNERSHIP to the data and information pertaining to their operations they report to crop insurance agencies, government agencies, vendors, and service providers.

2. U.S. Agriculture Producers have the RIGHT TO CLAIM OWNERSHIP to the data and information pertaining to their operations that originates, or is collected, on technology equipment they own or lease, regardless of how or where the data or information are transferred.

3. U.S. Agriculture Producers have the RIGHT TO CHOOSE the repository in which any and all data and information pertaining to their operations are stored.

4. U.S. Agriculture Producers have the RIGHT TO CONTROL the repository in which the data and information pertaining to their operations are stored.

5. U.S. Agriculture Producers have the RIGHT TO CONTROL with whom they will share data and information pertaining to their operations.

6. U.S. Agriculture Producers have the RIGHT TO CONTROL AND LIMIT what data and information pertaining to their operations are shared with third parties.
7. U.S. Agriculture Producers have the RIGHT TO DATA SECURITY technologies that meet or exceed international standards to protect the data and information stored in their repositories.

8. U.S. Agriculture Producers have the RIGHT TO MAINTAIN PRIVACY with regards to information or data that contain personal, financial, or geo-spatial information.

9. U.S. Agriculture Producers have the RIGHT TO PARTICIPATE in the monetization of the data and information pertaining to their operations.

10. U.S. Agriculture Producers have the RIGHT TO REMAIN INDEPENDENT by establishing — with government and agri-business — the precedent that they own and control the data and information pertaining to their operations.
APPENDIX D: Ag Companies Policies on Big Data / Data Privacy

This information reflects the publicly available big data / data privacy policies for ag companies.

DISCLAIMER: INFORMATION IS CURRENT AS OF THE DATE OF THIS WHITEPAPER, HOWEVER, WHERE AVAILABLE LINKS TO THE WEBSITE HAVE BEEN PROVIDED TO ENABLE THE READER TO JUMP TO THE MOST CURRENT VERSION OF THE POLICY OR PRACTICE.
CNH INDUSTRIAL

Updated: June 12, 2014

CNH Industrial Data Ownership & Data Access – Guiding Principles

CNH Industrial, through its agricultural brands Case IH and New Holland, offers a full range of agricultural equipment to farmers around the world. For almost 20 years CNH Industrial’s brands have been offering advanced precision technologies to help farmers use their data to farm better and smarter.

Over this period of time our customers have been using these technologies to reduce input cost, improve yields, and increase efficiencies. However, as precision technologies have evolved, so has the need for better methods to manage data access and the need for more customer-controlled and customer-owned data.

Along with technological improvements, CNH Industrial has developed a series of guidelines and principles to follow in regards to data ownership and access.

CNH Industrial is committed to:

- **Farmer-Owned Data Systems** – All data generated or entered by the farmer, their employees, or by machines is controlled by the customer, while utilizing open industry standards for secure data sharing. This allows producers to realize the full value of their data and the right to select what can be shared and with whom.

- **Safe and Secure Data Systems** – The systems are designed to be secure in maintaining or transmitting information so as to not compromise the producer’s privacy or sensitive information.

- **Integrated and Open Data Systems** – Should they choose, farmers are able to share data with CNH Industrial or third-parties through a system that incorporates technologies which allow and require growers to identify which data may be shared thus reducing complexity by providing a platform for farmers to seamlessly and simply leverage the data they produce.

- **Evolving Data Systems** – Data systems will comply with industry standards for data communications yet be able to change as the needs and access for agricultural data expand and evolve.
CNH Industrial Data Access – Guidelines

- The data created by a farmer, or generated from equipment the farmer owns or leases, is owned by that farmer and should be easily accessible.
- All agronomic and non-proprietary machine performance data that is present on CNH Industrial machine data communication systems should be available to the grower in an unrestricted and easily accessible manner.
- All grower data will be private and secure.
- CNH Industrial will enable the grower to select which data can be shared and who can access this data.
- Proprietary, often encrypted, machine-controlled data, such as the data flowing between an engine controller and a transmission controller, will not be made directly available to the grower to prevent “reverse engineering” of a CNH Industrial machine or modifications to the onboard machine messages which could result in the modification of controls which are in place to protect the operator and the machine.
- CNH Industrial will not sell data which can be identified to a specific location or grower to third parties.
- Any direct or indirect compensation for the use of growers’ data will be managed by the grower directly with the third party wishing to utilize this data. The market, not CNH Industrial will dictate the compensation/value for the data.
- CNH Industrial may, with the growers express permission, share aggregated data which is not identifiable to a specific grower or location to third parties.
- CNH Industrial will use, with the grower’s permission, machine performance data and encrypted proprietary machine operational data to develop and deliver machine diagnostics, machine maintenance and machine support services for delivery through CNH Industrial and its dealers.
- CNH Industrial will use machine performance data and encrypted proprietary machine operational data for internal product development purposes to improve both the setup and design of current and future products.
- CNH Industrial data systems will comply with industry standards such as ISO11783 for data communications.
- CNH Industrial will implement data sharing technology established by the Open Ag Data Alliance.
CLIMATE CORPORATION

http://www.climate.com/company/privacy-policy/

Last Updated June 3, 2014.

The Climate Corporation and its affiliates value the privacy and security of the information that our customers ("customers" or "you") choose to share with us through their purchase, enrollment or use of our farm management and decision support software, precision agriculture services and software, Precision Planting farming equipment, and insurance services, and our technology platforms, applications, and services insofar as they are used to deliver and support those products and services, which are described at www.climate.com/privacy-policy/products, (collectively, the "Climate Corporation Service Platform").

Please read this Privacy Policy carefully before you use the Climate Corporation Service Platform so that you will understand our practices and your options before you choose to share your information. Your use of the Climate Corporation Service Platform means that you agree to our collection, use, and disclosure of the information you share with us, as explained in this Privacy Policy.

YOUR OWNERSHIP OF YOUR INFORMATION

We presume you own the information and data that you provide to us when you purchase, set up an account for, or use any Climate Corporation Service Platform product or service, including, for example, the data generated from the farming equipment you own or lease (collectively, “Your Information”). We do not claim any ownership interest in Your Information. That means that as between you and us, Your Information remains yours even after you provide it to us. By providing Your Information, you represent that you have the right to share it with us and to allow us to use and disclose it as explained in this Privacy Policy.

YOUR INFORMATION

Information We May Collect From You

As a Climate Corporation Service Platform customer, we may collect from you the following information:

For Insurance Products

- Name, address and telephone number
- Email address
- Date of Birth
- Social Security Number
- Credit or consumer reporting or history
- Field location
- Browser and device information
- Demographic information
- Information related to administering your coverage or claims
- Information about your farming operations
For All Other Products

- Name, address and telephone number
- Email address
- Field location
- Browser and device information
- Demographic information
- Information about your farming operations

You may also provide to us your credit card number, debit card number, or bank account information, depending on how you choose to pay for Climate Corporation Service Platform products and services.

How We May Use and Share Your Information

We may use Your Information:

- to deliver, administer and enhance Climate Corporation Service Platform products and services that you purchase or use ("Your Products");
- to communicate with you about Climate Corporation Service Platform products and services, subject to your right to opt out at any time; and
- for other purposes to which you expressly consent.

Other than for those permitted uses, we will not share Your Information:

- with any governmental entities, unless compelled or legally required, in our judgment, to do so; or
- with others without your consent, except with Service Providers.

"Service Providers" are the companies and consultants that we work with to support our Climate Corporation Service Platform operations, who agree not to use or disclose Your Information other than to provide services for us or as required by law. Examples include companies and consultants that provide website hosting, software development, payment processing, order fulfillment, information technology and related infrastructure support, customer service, email delivery, credit card processing, legal and financial advice, and auditing. For insurance customers, Service Providers also may include your insurance agent and agency, the issuing insurer of your policy, claim and investigation service providers, fraud prevention service providers and their respective attorneys.
AGGREGATED INFORMATION

“Aggregated Information” is a combination and analysis of information from multiple sources that helps identify or creates trends, benchmarks, summary metrics, or predictive algorithms, provided that we take reasonable steps to prevent a specific individual or the individual’s data from being identified. We may create Aggregated Information from information that other customers choose to share with us, along with Your Information. Examples of Aggregated Information include summary pest and disease reports for a customer’s region, average yield by practice in a customer’s county, average input costs for all growers in a customer’s state, a soil moisture estimate for a particular soil type, or a yield improvement estimate for a particular farming practice decision.

We may use Aggregated Information:

- to deliver, administer, develop and enhance Climate Corporation Service Platform products and services;
- to enable general marketing and advertising statements about our products and services; and
- for other purposes to which you expressly consent.

OTHER INFORMATION USE AND DISCLOSURE RIGHTS AND COMMITMENTS

We further commit that:

- We will not use Your Information or Aggregated Information for seed pricing.
- We will not use Your Information or Aggregated Information to make speculative commodities trades, although we may use financial derivative instruments and natural hedges to limit exposure to changes in foreign currency exchange rates, commodity prices and interest rates.
- We will not sell Your Information to third parties.

We may also use or share Aggregated Information as we believe to be necessary or appropriate:

- to comply with applicable laws or legal process; and
- to protect our legal rights, such as pursuing available remedies or limiting the damages we may sustain.

MARKETING AND ADVERTISING

How we may use Your Information for marketing and advertising

We will not use Your Information to promote or advertise any third party’s products or services without your consent. If you provide consent, then you may opt out at any time.

We may use Your Information to communicate with you about our products and services, subject to your right to opt out as explained below.
Opting out of marketing communications

You may opt out from receiving Climate Corporation Service Platform paper marketing communications by contacting our Customer Support center at support@climate.com or 1-888-924-7475. You may opt out from receiving Climate Corporation Service Platform marketing emails by following the instructions in the email you receive. Please note that we may still send you important administrative messages related to your use of Your Products, from which you cannot opt out.

**CHOICES AND ACCESS**

**Ability to delete Your Information**

We intend to give you the ability to delete any of Your Information and accounts for Climate Corporation Service Platform products and services at any point, and our intention is that once you make the request and we have acted on it, Your Information will no longer be available to us as described in this Privacy Policy. Any such data will, however, be preserved in a restricted archive in the event that you wish to request the data in the future. We will permanently delete the data after approximately twelve (12) months of the deletion request, although we will permanently delete the data sooner if you ask us to do so.

There are some limitations on your ability to have Your Information deleted. Specifically, you will not be able to delete Your Information that:

- has been incorporated into Aggregated Information; or
- we are using it to support your use of Your Products at the time you ask to have it deleted.

In addition, we may not delete certain information if retaining it is, in our reasonable judgment, necessary or appropriate: (i) to comply with applicable laws or legal process or (ii) to protect our legal rights, such as pursuing available remedies or limiting the damages we may sustain. Also, please note that if we have information available to us from sources other than your submissions through the Climate Corporation Service Platform, the fact that you request deletion of information you submitted may not mean that all matching information from other sources will also be deleted.

If you would like to ask us to delete Your Information (aside from the deletion exceptions above), you may contact us by email at delete-request@climate.com. In your request, please make clear what information you would like to have deleted. For your protection, we may only implement requests with respect to the information associated with the particular email address that you use to send us your request, and we may choose to take other steps to verify your identity before implementing your request. We will try to comply with your request as soon as reasonably practicable.
Ability to easily share Your Information

We want our customers to have control over their data and freedom to move their data to any company they trust. We will continue to work hard to make this possible through an open authorization model, as described by OADA (see www.openag.io for more information).

In addition, we may make it possible for you to share your specific account information directly with other customers and users. This will only be possible if you explicitly authorize us to do so and authenticate your identity. You may delete this authorization at any time.

Ability to request certain insurance policy information

As an insurance policyholder, you can always review and update your information through your online account at www.climate.com or by calling our Customers Support center at 1-888-924-7475. If you have questions about the information in your insurance policy file (with the exception of certain documents relating to claims, investigations, litigation and disputes), please contact us and we will respond within thirty (30) business days. If you believe any information is incorrect, we will investigate and, if appropriate, correct the information.

DATA SECURITY

We use reasonable organizational, technical and administrative measures to protect Your Information. If you have reason to believe that your interaction with us is no longer secure, please immediately notify us in accordance with the “Contacting Us” section below.

Protection of Social Security Numbers: With respect to Climate Corporation Service Platform products and services for which we collect Social Security numbers, it is our policy to: (1) protect the confidentiality of such numbers; (2) prohibit their unlawful disclosure; and (3) limit access to them.

To protect your privacy and security, we take certain steps designed to verify your identity before granting customer account access. You are responsible for maintaining the secrecy of your unique password and account information at all times and for any transactions performed from that account.

INDEPENDENT AUDITS OF OUR PRIVACY POLICY COMPLIANCE

We mean what we say in this Privacy Policy. Accordingly, we will engage regular independent third party audits of Climate Corporation Service Platform systems and procedures to confirm adherence to this Privacy Policy, and we will publish the resulting audit reports.
USE OF ONLINE SERVICES BY MINORS

The Climate Corporation Service Platform and related Online Services are not directed to individuals under the age of eighteen (18), and we request that these individuals not provide us with any of their information or use our Online Services.

CROSS-BORDER TRANSFER AND INTERNATIONAL USERS

The Online Services are controlled and operated by us from the United States, and are not intended to subject us to the laws or jurisdiction of any state, country or territory other than those of the United States. Your Information may be stored and processed in any country where we have facilities or in which we engage service providers, and by using the Climate Corporation Service Platform, you consent to the transfer of information to countries outside of your country of residence, including the United States, which may have different data protection rules than those of your country.

ONLINE INFORMATION

We may collect Your Information through your use of online Climate Corporation Service Platform services, websites, and applications (“Online Services”), including as follows:

- **Through your browser or device:** When you use any Online Service, certain information is collected by most browsers or automatically through your device, such as your Media Access Control (MAC) address, computer type (Windows or Macintosh), screen resolution, operating system name and version, device manufacturer and model, language, Internet browser type and version and the name and version of the Online Services you are using. We use this information to ensure that the Online Services function properly.

- **Through your use of mobile applications:** When you download and use any Climate Corporation Service Platform mobile application (each, an “App”), we and our service providers may track and collect App usage data, such as the date and time the App on your device accesses our servers and what information and files have been downloaded to the App based on your device number. We and our service providers use the App information for security purposes, display information more effectively, and to personalize your experience while using the Apps. We also gather statistical information about the usage of the Apps in order to continually improve their functionality, understand how they are used and resolve questions regarding them.

- **Using cookies and similar technologies:** Cookies are pieces of information stored directly on the computer you are using. Cookies allow us to collect information such as browser type, time spent on using our, pages visited, language preferences, and other anonymous traffic data. We and our service providers use the information for security purposes, to facilitate navigation, display information more
effectively, and to personalize your experience while using the Online Services. We also gather statistical information about the usage of the Online Services in order to continually improve their functionality, understand how they are used and resolve questions regarding them. If you do not want information collected through the use of cookies, there is a simple procedure in most browsers that allows you to automatically decline cookies or be given the choice of declining or accepting the transfer to your computer of a particular cookie (or cookies) from a particular site. You may also wish to refer to http://www.allaboutcookies.org/manage-cookies/index.html. If, however, you do not accept cookies, you may experience some inconvenience in your use of the Online Services. For example, we may not be able to recognize your computer and you may need to log in every time you visit the applicable Online Services.

- **Using pixel tags and other similar technologies.** Pixel tags (also known as web beacons and clear GIFs) may be used in connection with some Online Services to, among other things, track the actions of users of the Online Services (including email recipients), measure the success of our marketing campaigns and compile statistics about usage of the Online Services and response rates.

- **IP Address:** Your IP Address is a number that is automatically assigned to the computer that you are using by your Internet Service Provider (ISP). An IP Address may be identified and logged automatically in our server log files whenever a user accesses the Online Services, along with the time of the visit and the page(s) that were visited. Collecting IP Addresses is standard practice and is done automatically by many websites, applications and other services. We use IP Addresses for purposes such as calculating usage levels of the Online Services, helping diagnose server problems, and administering the Online Services.

- **Physical Location:** We may collect the physical location of your device by, for example, using GPS, cell phone tower or WiFi signals. We may use your device’s physical location to provide you with personalized location-based services and content. In some instances, you may be permitted to allow or deny such uses and/or sharing of your device’s location, but if you choose to deny such uses and/or sharing, we may not be able to provide you with the applicable personalized services and content.
THIRD PARTY SERVICES AND USER-GENERATED CONTENT

This Privacy Policy does not address, and we are not responsible for, the information collection, use, disclosure or security policies or practices by, the information provided by, or other practices of any third party. That includes, for example:

- any third party operating any site or service to which any Online Service links;
- any other app developer, app provider, social media platform provider, operating system provider, wireless service provider, or device manufacturer, including, for example, Facebook, Apple, Google, or Microsoft; and
- any channel partner and other user to whom you provide Your Information or Climate Corporation Service Platform account access. That may include, for example, the dealers, insurance agents and sales representatives who participate in your purchase or use of Your Products. We will allow you to view who has that access and revoke access upon request.

We are not responsible for the information, including personally identifiable information, that you submit in any user-generated content services, such as posting a question, answer, or blog on any public facing portion of the Climate Corporation Service Platform. Any personally identifiable information you submit there can be read, collected, or used by other users and could be used to send you unsolicited messages.

The inclusion of a link on an Online Services does not imply endorsement of the linked site or service by us.

UPDATES TO THIS PRIVACY POLICY

We may change this Privacy Policy. The “Last Updated” legend at the top of this page indicates when this Privacy Policy was last revised. Any changes to this Privacy Policy will become effective when we post or distribute the revised Privacy Policy. Your use of the Climate Corporation Service Platform following these changes means that you accept the revised Privacy Policy.

CONTACTING US

If you have any questions about this Privacy Policy, please contact us at legal@climate.com or:

Legal Department  
The Climate Corporation  
201 Third Street, Suite 1100  
San Francisco, CA 94103

Because email communications are not always secure, please do not include credit card information or other sensitive information in your emails to us.
Our Commitment to Customer Business Data

John Deere believes that insights from data will be a key part of meeting our industry's collective goal to produce enough food and to build the infrastructure required to sustain a growing world population. We also believe that companies providing data services should have effective processes that ensure privacy, security and control for their customers.

Keeping your trust is important to us, so we developed a set of Business Data Principles and Frequently Asked Questions that reflect our core values of integrity, quality, commitment and innovation. These emphasize our commitment to building a secure data sharing and storage platform based on three principles:

- **Value** – The data you create has value and if you choose to share it, we believe that value can grow.
- **Transparency** – We want you to understand what we do, why we do it and what it means to you.
- **Control** – You are in control of the data that's collected and with whom it is shared. That's why you must give your permission before John Deere shares your data with anyone.

These principles will guide John Deere's decisions as we continue the relationship we've been building with our customers for more than 175 years.

http://www.deere.com/wps/dcom/privacy_and_data/privacy_and_data_services_subscriptions_data_policy_US.page

John Deere Data Services and Subscriptions Data Policy Statement for the United States

Effective Date: May 9, 2014

This policy explains the types of business information that we collect through the John Deere Data Services and Subscriptions and how we may use and disclose this information. It provides information about how we maintain, use, disclose and protect your business information. It also describes your options in the event you do not want us using or disclosing your business information for certain purposes in the future. The “Data Services and Subscriptions” governed by this policy are the MyJohnDeere.com websites together with JDLink and the other offerings with customer agreements listed for the United States at www.deere.com/agreements.

1. **How we classify and use your business data.** When hosting or managing business data that you bring to us, we distinguish among Production Data, Machine Data, and Other Data:

   Production Data is information specific to the work our customers do with their equipment and the land on which the work is performed. For example, field task details, material moved, crop harvested or agronomic inputs applied. We use Production Data only as follows:
We, and our service partners, affiliates and suppliers, use Production Data to provide you with contracted services and offerings and to administer your account.

We may anonymize Production Data to create anonymized data sets, unless you indicate that we may not do so via the MyJohnDeere.com account management options. Please note that we consider any anonymized datasets that result from our anonymization processes to be proprietary to John Deere. John Deere will be free to use, sell and disclose the anonymized datasets, and John Deere may offer or sell information and services that are derived from the anonymized datasets. If you choose to opt out of this data anonymization, your choice will apply prospectively only and John Deere will have no obligation with respect to any anonymized datasets that were generated prior to your opt-out selection.

John Deere may disclose Production Data to comply with court orders and legal or regulatory requirements; to prevent injury, death, losses, fraud or abuse; to protect John Deere’s rights or to defend John Deere in legal proceedings; and to comply with requests from you.

Machine Data is information associated with how equipment is functioning. Examples include fuel consumption, machine health indicators, diagnostic codes and engine performance. We use Machine Data only as follows:

We, and our service partners, affiliates and suppliers, use Machine Data to provide you with contracted services and offerings and to administer your account.

We, and our service partners, affiliates and suppliers, may use Machine Data to develop and improve products and services.

We may share Machine Data with John Deere dealers so that they can support you, unless you affirmatively restrict access to specific dealers via the MyJohnDeere.com account management options.

We may anonymize Machine Data to create anonymized data sets, unless you indicate that we may not do so via the MyJohnDeere.com account management options. Please note that we consider any anonymized datasets that result from our anonymization processes to be proprietary to John Deere. John Deere will be free to use, sell and disclose the anonymized datasets, and John Deere may offer or sell information and services that are derived from the anonymized datasets. If you choose to opt out of this data anonymization, your choice will apply going forward only, and John Deere will have no obligation with respect to any anonymized datasets that were generated prior to your opt-out selection.

John Deere may internally use, view or research Machine Data to identify trends for statistical analysis, in connection with warranty, product support and for diagnostic or prognostic purposes.
John Deere may disclose Machine Data to comply with court orders and legal or regulatory requirements; to prevent injury, death, losses, fraud or abuse; to protect John Deere’s rights or to defend John Deere in legal proceedings; and to comply with requests from you.

Other Data is information used by John Deere only to support you. Examples include variable rate prescriptions, user-entered notes and user-formatted reports. We do not anonymize Other Data for external sharing even if you opt to allow John Deere to anonymize Machine and Production Data for external sharing. We use Other Data only as follows:

- We, and our service partners, affiliates, and suppliers, use Other Data to provide you with contracted services and offerings and to and administer your account.

- John Deere may disclose Other Data to comply with court orders and legal or regulatory requirements; to prevent injury, death, losses, fraud or abuse; to protect John Deere’s rights or to defend John Deere in legal proceedings; and to comply with requests from you.

For examples of data and information that falls within these categories, please view our Data Type Inventory, available at: http://www.deere.com/privacy_and_data/docs/DataTypeInventory.pdf. As between you and John Deere, you are responsible for ensuring that you have the right to transfer and license any data that you bring to John Deere via the Data Services and Subscriptions for the uses described above.

Please note that in this Data Policy Statement, “Machine Data” is defined more narrowly than it is in tab 2 of our Enterprise Privacy Statement (available at www.deere.com/legal). This narrower definition governs our use and management of your business data with respect to the Data Services and Subscriptions.

2. You control who sees your business data. You control the business data you bring to us, subject to John Deere’s rights of use identified above:

- Sharing. You may share and disclose data within MyJohnDeere.com. As noted above, you control which dealers have access to data in your account; and you also control other parties’ access and visibility into the data in your account.

- Managing. You may view, analyze and download some data in your account via the MyJohnDeere.com and JDLink.com portals.

- Deletion. You may request that we delete Machine Data, but doing so may limit our ability to support you; and in some cases may constitute a termination under the terms of any applicable Data Service and Subscription contracts between you and us (please review the terms of any such contract for details). You may delete Production and Other Data directly via www.MyJohnDeere.com or by asking your dealer to contact us on your behalf. Please note that, unless you delete your business data as provided above, John Deere may, but is not obligated to, retain the data indefinitely. After expiration of
any applicable Data Service and Subscription contract, we may delete data at our discretion and subject to requirements in applicable privacy, consumer protection or other laws.

3. **How we protect your business information.** We understand the need to safeguard business information that you provide to us. We have implemented and will maintain standards and procedures designed to prevent misuse of that information. We maintain physical computer and network security. We educate our employees about the importance of data security and customer service through standard operating procedures and special training programs. We maintain security standards and procedures to help prevent unauthorized access to information about you and we update and test our technology to improve the protection of your business data. We comply with all applicable laws, including data privacy and consumer protection laws. Please note that we may move data across jurisdictions and may store your business data outside your home country, including in the United States.

Last Updated: 9 May 2014
MONSANTO


Policy Last Updated May 2014

Monsanto Company values the privacy of individuals who visit the web sites which are operated throughout the world by Monsanto or its subsidiaries and adheres to the privacy standards which have been adopted by the countries in which Monsanto companies operate. This statement sets forth the important information which individuals who visit these sites need to know about how Monsanto companies collect and use personal information from web site visitors.

In this Privacy Policy, "Monsanto" refers to Monsanto Company and its subsidiaries and affiliates, including the business unit of Monsanto that operates the web site on which this Privacy Policy is found.

Please read this policy carefully. By visiting a Monsanto web site and using the services provided on that site, you are indicating your agreement to Monsanto’s use of your personal information as set out in this Policy.

This Policy is intended to be in compliance with the applicable privacy laws and regulations of each country in which Monsanto operates and from which personally identifiable information is collected. To the extent the laws of a country may prohibit Monsanto from using and sharing personal information in a way described in this Policy, the Policy and Monsanto’s practices shall be deemed modified to be consistent with such local laws.

What Does This Policy Cover?

This Privacy Policy applies to Monsanto web sites and information collected by and through those web sites. It does not apply to any other Monsanto services or dealings with users or customers and does not apply to third-party sites which may be linked to the Monsanto site.

Collection of Information

Monsanto web sites collect personally identifiable information only from individuals who voluntarily choose to provide the information through the web site. (In this Policy the foregoing information is referred to as "Personal Information.") That Personal Information may be collected in several different ways:

- Some sites may permit users to request a "user i.d." and password which can be used on future visits to the site. Visitors to the site may be asked to supply their name, geographic location and some information about their business or occupation or other reason for interest in the site. In addition, some sites permit users to supply an e-mail address to sign up for Monsanto newsletters. Other sites may include feedback or comment forms whereby users can submit questions or comments to Monsanto. (In this Policy, the foregoing information is referred to as "User Information.")
- Some sites may permit users to enter into transactions with Monsanto or to take advantage of services provided by Monsanto to its customers through that site or through its offices around the world. On
such sites, users will be required to provide detailed information necessary to enable Monsanto to process the transaction and to provide the goods or services requested by the visitor. Visitors may be requested to provide financial information, including credit card or bank information, in connection with such transactions. Visitors may also be asked to provide information about the pesticide and other licenses which they hold in order to determine whether Monsanto can lawfully sell the products requested by the visitor. (In this Policy, the foregoing information is referred to as "Transactional Information.")

- Some Monsanto web sites may provide chat rooms or discussion forums where users may register and post messages or comments. Participation in such discussion areas is entirely voluntary. No information which a user posts in such an area is private, inasmuch as it will be accessible to other users of the same area. Thus, any Personal Information which a user chooses to post in such an area will not be subject to this Privacy Policy.

- From time-to-time our site may request additional information from users by means of surveys or contests. Participation in these surveys or contests is completely voluntary and the user therefore has a choice whether or not to disclose whatever additional information may be requested. Information requested through surveys and contests may include additional demographic information. (In this Policy, the foregoing information is referred to as "Survey Information.")

In addition to the foregoing Personal Information, each site automatically logs information about a visitor from the browser used to access the site (e.g., Internet Explorer, Netscape, etc.). This includes information about the I.P. address of the visitor, the pages in the site which are visited from that address and the web site which the user visited just prior to the Monsanto site. (In this Policy, the foregoing information is referred to as "Visit Information.") While some jurisdictions consider IP addresses to be personal information, none of this Visit Information is used by Monsanto for direct or indirect identification of the individual user who is accessing the Monsanto site. Visit Information will be used by Monsanto to diagnose problems with its web servers, to administer, design and construct its web sites, to track visitor movements on the web sites and gather broad demographic information for aggregate use only.

Cookies

A cookie is a small data file that web sites commonly write to the site visitor's hard drive when a site is visited. A cookie file contains information that can identify a return visitor each time he or she visits our site. The data is encrypted for added security. Monsanto's web sites may use cookies as a way to measure activity and traffic patterns on the site in order to continually improve the visitor's experience. Cookies also provide visitors the convenience of not having to log in a password more than once on a Monsanto site, thereby saving the visitor time while on our site.

A browser can be set to warn the users before accepting cookies. Users can choose to refuse cookies by turning them off in the browser. Users do not need to have cookies turned on to visit our web site, but will need them to use certain customizable features of our web site such as automatically displaying local weather and crop forecasts, accessing certain areas of our web site, and transacting business on our web site.
While we take all reasonable steps to protect the privacy of our website visitors, we cannot promise that the current limitations of our online applications programming will address every browser setting or honor every personal browser preference. In particular, we have not implemented the necessary program changes to honor "Do Not Track" or "DNT" browser signals. As our online applications programming is refined, we will take all reasonable steps to honor such requests in the future. Please return to this privacy policy for further updates on this topic.

Further, our online service providers or business partners may implement technologies that allow for the collection of personally identifiable information over time and across websites. We recommend that you review each privacy policy posted on the websites that you visit to better understand privacy practices on those websites.

Monsanto's Use of Your Personal Information

Your Personal Information may be used to communicate with you about your use of our sites, to let you know about changes to our services or our site or to provide services to you or to improve our understanding of what visitors want and need to see on the sites. In particular:

- **User Information** may be used by Monsanto primarily to enhance the usability and friendliness of the Monsanto web sites and to ensure that the information which is provided is timely and relevant and meets the needs of our visitors. Monsanto may also use the information which visitors voluntarily furnish through these sites to provide information and promotional material to persons who have visited the Monsanto sites and to process specific requests for information which visitors may make. (See "Opting In / Opting Out" below if you do not wish to receive such materials from Monsanto.)
- **Transactional Information** will be used by Monsanto to process and complete the transaction for goods or services requested by the visitor.
- **Survey Information** will be used in a manner similar to User Information but will be used primarily in aggregate form to provide Monsanto with information on customer needs, product design, market demand, etc.

Also, you should know that your Personal Information, as well as Visit Information collected at a Monsanto site, may be used by Monsanto security personnel if deemed necessary to protect Monsanto from a threat or other perceived security risk and such information may be shared with law enforcement authorities if appropriate.

Sharing and Disclosure of Your Information

Monsanto may share Personal Information with others for a number of purposes:

- We may provide contact information to our trade partners, advertisers and other interested parties so that they may contact you directly to furnish you information about their products and services. (As used in this Policy, "Trade Partners" means businesses not owned or operated by Monsanto but which provide compatible goods or services which may be desired by or potentially useful for visitors to the
Monsanto web sites.) (See "Opting In / Opting Out" below if you do not wish to receive such materials from Trade Partners.)

- We will provide aggregated data about products and services purchased, visitor interests, demographics and other information collected from our web site to our Trade Partners, advertisers and other interested parties so that they can learn what products and services are most popular to our customers. Aggregated data will be in anonymous group statistical form and not associated with any individual person.
- We may use a credit card processing company to bill web site visitors for products and services which they request.
- We may partner with other parties to provide specific services. When the user signs up for these services, we will share names or other contact information that is necessary for the third parties to provide these services. These parties will not be allowed to use personally identifiable information except for the purpose of providing these services.
- We also may share Personal Information about visitors to our web sites among its corporate affiliates and subsidiary companies for purposes related to the business of those affiliates and subsidiaries.
- Monsanto may also share Personal Information about web site visitors with third parties under the following circumstances:
  - When you consent to disclosure;
  - To comply with law, court orders, subpoena or legal process;
  - To enforce or apply Monsanto's agreements or protect Monsanto and its rights,
  - By operation of law, when such Personal Information is transferred as a part of sale of assets including the assets represented by this site; or
  - In the event that Monsanto, or substantially all of its assets, are acquired outside of the ordinary course of business, and such Personal Information may be one of the transferred assets.

Transfers of Information

Because Monsanto operates from its headquarters in St. Louis, Missouri in the United States of America and through subsidiary companies located in many countries around the globe, and because its web servers which host its web sites are located at numerous locations inside and outside the United States, it is possible that Personal Information about visitors may be transferred from one country to another. Such transfers will only occur in compliance with the applicable local law relevant to the source of the information.

When you furnish Personal Information to Monsanto through a Monsanto web site, you are also giving your consent to a cross-border transfer of that information.

Children and Privacy

Monsanto does not knowingly collect information from or about children age 13 and under without the consent of a parent or legal guardian.

Opting In / Opting Out
Upon registering at any Monsanto web site which collects Personal Information, visitors will be given an opportunity to determine whether they wish to receive promotional materials from Monsanto or from Trade Partners. The manner and method in which a Monsanto site permits users to opt out of receiving such materials will be described on the individual site collecting that Personal Information. If the user would like to "opt out" at a later time, he may do so by following the instructions on the site where the original request was made or the instructions contained in the e-mail messages delivering such materials to him.

Likewise, you may withdraw your consent to the collection or use of your Personal Information at any time by sending an email message to email.webguru@monsanto.com identifying yourself and describing the Personal Information which you believe has been collected through this site.

**Correction/Updating of Personal Information**

Each site which collects Personal Information will provide users with instructions regarding correcting or updating that Personal Information. Some sites may maintain a user account section where visitors can make corrections themselves; others may provide an email link or contact information to request us to make those changes; generally, user requests for an update of Personal Information will be honored within a reasonable time after we receive a request. However, no changes to personal information will be permitted where the change would result in incorrect information or would alter a transaction with us already completed.

**Retention of Personal Information**

Monsanto will periodically delete Personal Information collected from visitors to its web sites if it is no longer needed for any purpose for which the information may be used or disclosed under the terms of this Policy.

**Security**

Monsanto takes precautions to protect users' information. Our safeguards include technical means and policies and procedures that our staff is trained to follow. In any event in which a Monsanto web site is hosted by a third party, these safeguards shall also apply. If as a registered user you receive a password, you should keep it confidential because it is the key to access to the information held by Monsanto about you. If you leave your computer's internet browser running and someone else uses your computer, they will be able to access your account; thus, if your computer is not physically secure remember to shut down your browser before you leave it.

We try to reduce the likelihood of accidental disclosures and unintended access and modification of account information, but it is impossible to eliminate this possibility completely. When users submit sensitive information via the website, their information is protected both on-line and off-line.

When an enrollment or order form asks users to enter sensitive information (such as credit card number) that information is encrypted and is protected with the Secure Socket Layer (SSL) technology.
While Monsanto uses SSL encryption to protect sensitive information online, it also takes steps to protect user-information off-line. All of our users' information, not just the sensitive information mentioned above, is restricted in our offices. Monsanto employees are kept up-to-date on our security and privacy practices. Any time new policies are added, our employees are notified and/or reminded about the importance we place on privacy, and what they can do to ensure our customers' information is protected.

Protecting Your Own Privacy

Please keep in mind that whenever you voluntarily disclose personal information online - for example on message boards, through email, or in chat areas - that information can be collected and used by others. Ultimately, you are solely responsible for maintaining the secrecy of your passwords and/or any account information.

Changes to Policy

If Monsanto decides to change its privacy policies and practices, we will post those changes to our Privacy Policy on our web site in advance of the changes taking effect, so our users are always aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. If at any point we decide to use personally identifiable information in a manner different from that stated at the time it was collected, we will notify users. Users will have a choice as to whether or not we use their information in this different manner. We will continue to be able to use information in accordance with the Privacy Policy under which the information was collected.

Contacting Monsanto

Each Monsanto web site provides a Contact Us section to facilitate feedback from site visitors. Please use this facility to notify us if you have any questions, concerns or complaints about the manner in which your personal information has been collected or handled by Monsanto, or contact Monsanto's offices in your country.
PIONEER HI-BRED INTERNATIONAL, INC

https://www.pioneer.com/home/site/ca/privacy-statement/#security

Revised September 19, 2012

Pioneer Hi-Bred International, Inc. and its affiliates (“DuPont Pioneer”) are concerned about privacy issues and want you to be familiar with how we collect, use and disclose information. Together with DuPont Pioneer’s Global Information Privacy Policy, this Privacy Statement describes DuPont Pioneer practices in connection with information that we collect through websites and mobile applications owned and controlled by DuPont Pioneer (respectively, the “Site” and the “App”), as well as all other means where notice is legally required. By providing Personal Information to DuPont Pioneer, you agree to the terms and conditions of this Privacy Statement.

- **PERSONAL INFORMATION**
  - Personal Information DuPont Pioneer Collects
  - How We Use Personal Information
  - How Personal Information is Disclosed

- **NON-PERSONAL INFORMATION**
  - Non-Personal Information We Collect
  - How We Collect Non-Personal Information
  - How We Use and Disclose Non-Personal Information

- **IP ADDRESSES**
  - How We Collect IP Addresses
  - How DuPont Pioneer Uses and Discloses IP Addresses

- **INTEREST-BASED ADVERTISING**
  - THIRD PARTY SITES
  - THIRD PARTY ADVERTISERS
  - SECURITY
  - CHOICES AND ACCESS
    - How you can access, change or suppress your Personal Information

- **RETENTION PERIOD**
  - USE OF SITE BY CHILDREN
  - CROSS-BORDER TRANSFER
  - SENSITIVE INFORMATION

- **UPDATES TO THIS PRIVACY STATEMENT**

- **CONTACTING DUPONT PIONEER**
PERSONAL INFORMATION

Personal Information DuPont Pioneer Collects

"Personal Information" is information that identifies you as an individual, such as:

- Name;
- Postal address (including billing and shipping addresses);
- Telephone or fax number;
- Email address;
- Gender;
- Date of Birth
- Credit and debit card number;
- Banking information, such as account and routing numbers;
- Vendor Tax ID numbers;
- National ID numbers such as Social Security Numbers;
- Financial information when you apply for credit;
- Passwords and reminder questions/answers;
- Purchase history.

DuPont Pioneer collects Personal Information when you participate in various opportunities that we provide, for example:

- When you order a product or service or make a request.
- When you register your purchase of a DuPont Pioneer product.
- When you request credit for the purchase of DuPont Pioneer products and services.
- When you register for goods, services, subscriptions, technology forum, or other communications through the Site or App.
- When you participate in a contest, promotion, sweepstakes, rewards program, customer group, survey, or other promotion.
- When you participate in a blog, forum, or interact with DuPont Pioneer using social media or other electronic or digital communications.
- When we conduct market research, meet you at a trade show, or other event.
- When you apply for a job with DuPont Pioneer or to be an authorized DuPont Pioneer sales professional.

We may combine Personal Information that we collect about you with Personal Information you provide to DuPont Pioneer through other sources, such as product registrations, inquiries, or marketing events. We will use the combined Personal Information in accordance with this Privacy Statement for as long as it is combined.
How We Use Personal Information

We may use Personal Information for the following purposes:

- Respond to your inquiries and fulfill your requests, such as to send you e-mail alerts, text messages, and other written or electronic communications.
- Send you important information regarding the Site or App, changes to DuPont Pioneer’s terms, conditions, and policies, and/or other administrative information.
- Complete and fulfill your purchase, for example, to process your payments, have your order delivered to you, communicate with you regarding your purchase, and provide you with related customer service.
- Send you marketing communications that we believe may be of interest to you, including information about trade shows.
- Evaluate your requests for credit to purchase products and services offered by DuPont Pioneer.
- Personalize your experience on the Site by presenting products and offers tailored to you.
- Allow you to participate in sweepstakes, contests and similar promotions and to administer these activities. Some of these activities have additional rules, which could contain additional information about how we use and disclose your Personal Information, so we suggest that you read these rules carefully.
- Permit you to send messages to a friend through the Site or App. By using this functionality, you are telling DuPont Pioneer that you are entitled to use and provide DuPont Pioneer with your friend’s name and email address.
- Allow you to communicate and interact with others through the Site or App (for example, through a blog, message board, messaging functionality, chat functionality, profile, or other social media).
- Permit you to register and participate in technology forums and other events with DuPont Pioneer.
- Enable DuPont Pioneer business purposes, such as data analysis, audits, researching, and developing new products, enhancing DuPont Pioneer’s website, improving DuPont Pioneer’s services, making field notes, observations, and prescriptions, collecting and providing agronomic and farm management information, developing marketing events, identifying usage trends and determining the effectiveness of DuPont Pioneer’s promotional campaigns.
- As we believe to be necessary or appropriate: (a) under applicable law, including laws outside your country of residence; (b) to comply with legal process; (c) to respond to requests from public and government authorities including public and government authorities outside your country of residence; (d) to enforce DuPont Pioneer terms and conditions; (e) to protect DuPont Pioneer operations; (f) to protect DuPont Pioneer rights, privacy, safety or property, you or others; and (g) to allow DuPont Pioneer to pursue available remedies or limit the damages that we may sustain.
How Personal Information is Disclosed

Your Personal Information may be disclosed:

- Within the DuPont Group of Companies for the purposes described in this Privacy Statement. DuPont and the local affiliate with whom you are interacting are jointly responsible for the management of the jointly-used Personal Information.
- To DuPont Pioneer’s third party service providers who provide services such as website, database, and server hosting, data analysis, payment processing, order fulfillment, product distribution, infrastructure provision, IT services, customer service, email delivery services, credit card processing, auditing services, and other similar services to enable them to provide services.
- To third parties such as agents, distributors, retailers, and sales professionals to facilitate the sale and distribution of DuPont Pioneer products and services which may include marketing communications.
- To third party sponsors of sweepstakes, contests and similar promotions.
- To a third party that may offer you credit to purchase products or services offered by DuPont Pioneer.
- To identify you to anyone to whom you send messages through the Site.
- To a third party in the event of any reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of DuPont Pioneer business, assets or stock (including in connection with any bankruptcy or similar proceedings).
- As we believe to be necessary or appropriate: (a) under applicable law, including laws outside your country of residence; (b) to comply with legal process; (c) to respond to requests from public and government authorities including public and government authorities outside your country of residence; (d) to enforce DuPont Pioneer terms and conditions; (e) to protect DuPont Pioneer operations; (f) to protect DuPont Pioneer rights, privacy, safety or property, you or others; and (g) to allow DuPont Pioneer to pursue available remedies or limit the damages that we may sustain.
- By you, when you participate in features on a DuPont Pioneer Site or App that provide the opportunity to interact with DuPont Pioneer and others (for example a blog, message board, messaging functionality, chat functionality, profile, field observations databases and applications, or other social media). When you use these features you should be aware that any information you submit, including your name, location and e-mail address, may be publicly available to others. We are not responsible for any information you choose to submit through these features and we strongly discourage you from disclosing any sensitive Personal Information (such as health or credit card information) through these features. If you use these features, your Personal Information may remain on the Site or App even after you cease use of the Site or App.
NON-PERSONAL INFORMATION

Non-Personal Information We Collect

"Non-Personal Information" is any information that does not reveal your specific identity, such as:

- Browser information;
- Information collected through cookies, pixel tags and other technologies;
- Demographic information and other information provided by you;
- Aggregated information;
- Information about your agricultural operation, including, but not limited to:
  - Field specific data, such as GPS coordinates, soil type, moisture patterns, yield, products used, agronomic observations, management practices, inputs, such as herbicides, pesticides, and fertilizers.
- Weather information
- Preferences concerning how you receive information

How We Collect Non-Personal Information

DuPont Pioneer and DuPont Pioneer’s third party service providers may collect Non-Personal Information in a variety of ways, including:

- Through your browser: Certain information is collected by most browsers, such as your Media Access Control (MAC) address, computer type (Windows or Macintosh), screen resolution, operating system version and Internet browser type and version.
- Using cookies: Cookies allow a web server to transfer data to a computer for recordkeeping and other purposes. We use cookies and other technologies to, among other things, better serve you with more tailored information, to facilitate your ongoing access to and use of the Site, and to provide you with personalized marketing. If you do not want information collected through the use of cookies, there is a simple procedure in most browsers that allows you to decline the use of cookies. Some features of the Site may not work properly if you decline the use of cookies. To learn more about cookies, please visit [http://www.allaboutcookies.org/](http://www.allaboutcookies.org/)
- Using pixel tags, web beacons, clear GIFs or other similar technologies: These may be used in connection with some Site pages and HTML-formatted email messages to, among other things, track the actions of Site users and email recipients, measure the success of DuPont Pioneer marketing campaigns and compile statistics about Site usage and response rates.
- From you: Information such as your location, as well as other information, such as your preferred means of communication, is collected when you voluntarily provide this information. Unless combined with Personal Information, this information does not personally identify you or any other user of the Site or App.
- In the same ways we collect Personal Information, as described above.
• By aggregating information: Aggregated Personal Information does not personally identify you or any other user of the Site or App, (for example, we may use Personal Information to calculate the percentage of DuPont Pioneer users who have a particular telephone area code).

How We Use and Disclose Non-Personal Information

Because Non-Personal Information does not personally identify you, we may use and disclose Non-Personal Information for any purpose. In some instances, we may combine Non-Personal Information with Personal Information (such as combining your name with your geographical location).

If we combine any Non-Personal Information with Personal Information, e.g., when we combine information you provide upon registration with Non-Personal Information to provide you with targeted personalized marketing, the combined information will be treated by DuPont Pioneer as Personal Information.

IP ADDRESSES

Your “IP Address” is a number that is automatically assigned to the computer that you are using by your Internet Service Provider (ISP).

How We Collect IP Addresses

An IP Address is identified and logged automatically in DuPont Pioneer server log files whenever a user visits the Site, along with the time of the visit and the page(s) that were visited. Collecting IP Addresses is standard practice on the Internet and is done automatically by many web sites.

How DuPont Pioneer Uses and Discloses IP Addresses

DuPont Pioneer uses IP Addresses for purposes such as calculating Site usage levels, helping diagnose server problems, administering the Site and presenting content that is tailored to your country. We may also use and disclose IP Addresses for all the purposes for which we use and disclose Personal Information. Please note that we treat IP Addresses, server log files and related information as Non-Personal Information, except where we are required to do otherwise under applicable law.

INTEREST-BASED ADVERTISING

DuPont Pioneer and DuPont Pioneer third party service providers use cookies, pixel tags, web beacons, clear GIFs or similar technologies to track the actions of Site users and email recipients across non-affiliate websites over time, in order to personalize your experience on the Site by presenting advertisements that are more relevant to you. For example, we use third party service providers, to present products and offers tailored to the preferences and interests demonstrated by your online activity over time.

THIRD PARTY SITES

This Privacy Statement does not address, and we are not responsible for, the privacy, information or other practices of any third parties, including any third party operating any site to which the Site or the App contains
a link. The inclusion of a link on the Site or the App does not imply endorsement of the linked site by DuPont Pioneer.

THIRD PARTY ADVERTISERS

DuPont Pioneer may use third-party advertising companies to serve ads when you visit a DuPont Pioneer Site. Please note that these companies may use information about your visit to this Site in order to provide advertisements about goods and services that may be of interest to you. In the course of serving advertisements to this Site, these companies may place or recognize a unique cookie on your browser. If you would like more information about this practice and to know your choices about not having this information used by these companies, please visit http://networkadvertising.org/optout_nonppii.asp.

SECURITY

DuPont Pioneer uses reasonable organizational, technical and administrative measures to protect Personal Information under DuPont Pioneer control. Unfortunately, no data transmission over the Internet or data storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with DuPont Pioneer is no longer secure (for example, if you feel that the security of any account you might have with DuPont Pioneer has been compromised), please immediately notify DuPont Pioneer of the problem by contacting DuPont Pioneer in accordance with the "Contacting DuPont Pioneer" section below.

CHOICES AND ACCESS

Your choices regarding DuPont Pioneer’s use and disclosure of your Personal Information.

DuPont Pioneer gives you many choices regarding DuPont Pioneer’s use and disclosure of your Personal Information for marketing purposes. By visiting the DuPont Pioneer My Preferences page, you may opt-out from receiving future electronic marketing messages from DuPont Pioneer and request that we not share your Personal information with unaffiliated third parties for their marketing purposes.

We will try to comply with your request(s) as soon as reasonably practicable. Please note that if you opt-out as described above, we will not be able to remove your Personal Information from the databases of unaffiliated third parties with which DuPont Pioneer has already shared your Personal Information (i.e., to which we have already provided your Personal Information as of the date that we implement your opt-out request). Please also note that if you do opt-out of receiving marketing-related messages from DuPont Pioneer, we may still send you important administrative messages, and you cannot opt-out from receiving administrative messages.

How you can access, change or suppress your Personal Information

If you would like to review, correct, update, suppress, delete or otherwise limit DuPont Pioneer use of your Personal Information that has been previously provided to DuPont Pioneer, you may visit the DuPont Pioneer My Preferences page or contact support@pioneer.com.

In your request, please make clear what information you would like to have changed, whether you would like to have your Personal Information suppressed from a DuPont Pioneer database or otherwise let DuPont Pioneer
know what limitations you would like to put on DuPont Pioneer use of your Personal Information. We will try to comply with your request as soon as reasonably practicable.

RETENTION PERIOD

We will retain your Personal Information for the period necessary to fulfill the purposes outlined in this Privacy Statement unless a longer retention period is required or allowed by law.

USE OF SITE BY CHILDREN

DuPont Pioneer is committed to protecting the privacy needs of children and we encourage parents and guardians to take an active role in their children’s online activities. DuPont Pioneer does not target the Site or the App to children less than fourteen (14) years of age or knowingly collect information from children for the purpose of selling products or services. DuPont Pioneer does participate in select educational programs such as science and environmental awareness in support of schools and communities.

CROSS-BORDER TRANSFER

Your Personal Information may be stored and processed in any country where we have facilities or where we have engaged a service provider, and by using DuPont Pioneer Site or App you consent to the transfer of information to countries outside of your country of residence, including to the United States, which may have different data protection rules than in your country.

SENSITIVE INFORMATION

We ask that you not send DuPont Pioneer, and you not disclose, any sensitive Personal Information (e.g., information related to racial or ethnic origin, political opinions, religion or other beliefs, health, criminal background or trade union membership) on or through the Site or App or otherwise to DuPont Pioneer.

Employment applicants may be asked for information pertaining to criminal background as part of the hiring process to the extent allowed by applicable country law.

UPDATES TO THIS PRIVACY STATEMENT

We may change this Privacy Statement. Please note the document date at the bottom of this policy. Any changes to this Privacy Statement will become effective when we post the revised Privacy Statement on the Site or App. Your use of the Site or App following these changes means that you accept the revised Privacy Statement.

CONTACTING DUPONT PIONEER

If you have any questions about this Privacy Statement, please contact DuPont Pioneer at privacy@pioneer.com or by mail at
RAVEN INDUSTRIES

http://ravenind.com/privacy-policy/

Raven Industries, Inc. sole purpose for operating websites is to provide information concerning its services and products to customers, vendors, business partners, employees and others. We recognize the importance of maintaining the privacy of any personal information collected through the websites we operate. Therefore, visitors can reach us on the Web without revealing personal information. Visitors on the Web may elect to voluntarily provide personal information via websites, but are not required to do so, when filling out and submitting online questionnaires concerning feedback on the website, requesting information on products or services, or seeking employment. The personal information voluntarily provided by website users is contact information limited to the user’s email address solely for the purpose of answering questions and forwarding requested information. Raven does not sell or share this information with non-agent third parties.

Raven takes children’s privacy seriously. We do not knowingly collect personal information from children under the age of 13 through our website. If you are under 18 years of age, please don’t submit any personal information through our websites without the express consent and participation of your parent or guardian.

Website users who wish to request that Raven Industries not use information previously provided, correct information previously provided, or remove information previously provided to us may forward such requests to:

Raven Industries, Inc.

PO Box 5107 Sioux Falls, SD 57117-5107 raveninfo@ravenind.com

Requests should include the individual’s name, address, and other relevant information in order to correctly identify the user. We will use all reasonable efforts to honor such requests as quickly as possible. Raven websites may contain links to other “non-Raven” websites, and we assume no responsibility for the content or the privacy policies and practices on those websites. We encourage everyone to read the Privacy Policies of those sites as their privacy practices may differ.

In the event that any other website operated by Raven has different privacy policies, the privacy policies set forth on that website will govern the use of that site.

By using our website, you consent to our use of information that is collected or submitted as described in this online privacy policy. We may change or add to this privacy policy so we encourage you to review it periodically.