ZedX Privacy Policy

August 16, 2016

Table of Contents

ZedX Privacy Policy

1 EU-U.S. Privacy Shield

1.1 Introduction

The EU-U.S. Privacy Shield Policy (Policy) concerns the collection, use, retention, and security of personal information from European Union member countries.

ZedX, Inc. develops information technology products and services for the agricultural, environmental, and energy sectors. ZedX is committed to upholding the highest ethical standards in its business practices and strives to collect, use, and disclose personal information in a manner consistent with the laws of the countries in which it does business.

1.2 Compliance

ZedX, Inc. complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. ZedX has certified that it adheres to the Privacy Shield Principles (Principles) of (1) Notice, (2) Choice, (3) Accountability for Onward Transfer, (4) Security, (5) Data Integrity and Purpose Limitation, (6) Access, and (7) Recourse, Enforcement and Liability. If there is any conflict between the policies in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov .

This EU-U.S. Privacy Shield Policy sets forth the privacy principles that ZedX follows with respect to personal consumer information collected within the United States, and that transferred from the European Union (EU) to the United States. Accordingly, we follow the Principles published by the U.S. Department of Commerce at https://www.privacyshield.gov/EU-US-Framework with respect to all such data.

This Policy outlines our general practices for implementing these principles, including the types of information we gather, how we use it, and the notice and choice affected individuals have regarding our use of and their ability to correct that information.

1.3 Scope

This Policy applies to all personal information received by ZedX globally (including the United States and the EU), whether in electronic, paper, or verbal format.

1.4 Definitions

“Personal Information” or “Information” means information that (1) is received by ZedX from users in any part of the world, including information that is transferred from the EU to the United States; (2) is recorded in any form; (3) is about, or pertains to a specific individual; and (4) can be linked to that individual.

“Sensitive Personal Information” means personal information that reveals race, ethnic origin, sexual orientation, political opinions, religious or philosophical beliefs, trade union membership, or that concerns an individual’s health.

“Nonpublic Personal Information” is nonpublic information about you that we obtain in connection with providing services or information from the ZedX products and services to you and/or others. For example, nonpublic personal information includes information regarding your name, affiliation(s), location, history of data input or submissions, etc.

1.5 EU-U.S. Privacy Principles

1.5.1 Notice

Users of ZedX websites may elect to provide personal information to ZedX via e-mail, online registration forms, verbal conversations on the telephone, or other mechanisms applicable to use of the website. In addition, users may be required to provide ZedX with certain information in order to gain access to the website. This information is used internally, as appropriate, to handle the sender's requests, billing purposes, and other matters pertaining to operation of the website. ZedX will not knowingly disclose, sell, lease, rent, or sublicense this information to any third party.

ZedX may also use this information to create summary statistics, to determine the level of interest in information available on the website, and to improve user interaction.

Some ZedX websites may use a "cookie" temporarily stored in the visitor's computer memory (RAM) to allow the web server to log the pages you use within the website and to know if you have visited the website before.

Protecting your privacy is important to ZedX. We want you to understand what information we collect and how it is used and shared with others. In order to provide users with a broad range of information and services as effectively and conveniently as possible, ZedX uses various technologies to manage information submitted to our websites.

ZedX may collect Nonpublic Personal Information about you from the following sources:

- Information received from you regarding the setup of your access to the website;
- Information about your transactions on the website while visiting the website, as well as transaction with any related products or services offered by ZedX;
- Information or data you submit to the website for processing, and
- Information we receive from third parties responsible for disseminating your information or from whom you receive other products or services.

Nonpublic Personal Information collected includes your name, affiliation(s), job title, address, phone, cell phone, fax, email, and history of data input or submissions. This information is used for account management purposes.

Individuals subscribing to ZedX services have access to their personal data in their own account page within the website for viewing and editing addresses, phone numbers, etc. Subscribers have the choice and means for limiting the use and disclosure of their Personal Information. Section 1.5.7, Recourse, Enforcement, and Liability, provides contact information.

If you decide to stop using our website, we will continue to adhere to the privacy policies and practices described in this notice.

1.5.2 Choice

ZedX offers individuals the opportunity to choose (opt out) whether their Personal Information is (1) to be disclosed to a third party or (2) to be used for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual. Currently, ZedX does not transfer personal information to third parties.

ZedX does not collect Sensitive Personal Information for its products and services. In the event that ZedX would collect Sensitive Personal Information for its products and services, it will give individuals the opportunity to affirmatively or explicitly (opt out) consent to the disclosure of this information for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual. Individuals can use the contact information in section 1.5.7 to opt-out of the disclosure of this information. ZedX shall treat Sensitive Personal Information received from an individual the same as the individual would treat and identify it as Sensitive Personal Information.

1.5.3 Accountability for Onward Transfers

ZedX does not transfer personal information to third parties. In the event that our company would begin such transfers, ZedX will comply with the Notice and Choice Principles when transferring personal information to a third party. A contract will be made with the third party that provides such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles.

ZedX will verify that the third party is in compliance, and take the appropriate steps to stop and remediate unauthorized handling of personal information. ZedX will provide a copy of its privacy provisions to the Department of Commerce upon request. In cases of onward transfer to third parties of data of EU individuals received pursuant to the EU-US Privacy Shield, ZedX is potentially liable.

1.5.4 Security

ZedX has taken steps to safeguard information about users of our websites. We restrict access to your personal information to those employees who need to know that information to provide information or services to you. We maintain physical, electronic, and procedural safeguards that comply with industry standards to guard your nonpublic personal information from unauthorized disclosure.

The internet service by which our websites are made available brings together a combination of industry-approved security technologies to protect data for the operator and for the users of the websites. It features user name and password-controlled system entry, Secure Sockets Layer (SSL) protocol for data encryption, and a firewall to regulate the inflow and outflow of server traffic.

To access ZedX websites, you may be required to use log-on procedures established by the operator to begin a session of interaction with the site. Once the server session is established, the user and the server are in a secured environment. Data traveling between the user and the server is encrypted with Secure Sockets Layer (SSL) protocol. With SSL, data that travels between you and the site is encrypted and can only be decrypted with the public and private key pair (an industry standard). The server hosting the site issues a public key to the user's browser and creates a temporary private key. These two keys are the only combination possible for that session. When the session is complete, the keys expire and the whole process starts over when a user establishes another server session.

Requests for data transmission to ZedX websites must filter through a firewall before they are permitted to reach the server. The firewall blocks and directs traffic coming to the server. The configuration begins by disallowing ALL traffic and then opens communication links only when necessary to process acceptable data requests, such as retrieving web pages or sending user requests for information or processing to the website.

1.5.5 Data Integrity and Purpose Limitation

ZedX shall only process Personal Information in a way that is compatible with and relevant for the purpose for which it was collected or authorized by the individual. To the extent necessary for those purposes, ZedX shall take reasonable steps to ensure that Personal Information is accurate, complete, current, and reliable for its intended use. We may be required to disclose an individual's personal information in response to a lawful request by public authorities, including to meet national security or law enforcement requirements.

1.5.6 Access

Individuals have the right to access their data. ZedX shall allow an individual reasonable access to their Personal Information and allow the individual to correct, amend, or delete inaccurate information. Users with login access to ZedX websites can use their My Account or User Preferences links within the site to view or make changes to their Personal Information.

1.5.7 Recourse, Enforcement, and Liability

ZedX uses a self-assessment approach to assure compliance with this Policy and periodically verifies that it is accurate, comprehensive for the information intended to be covered, prominently displayed, completely implemented, accessible, and in conformity with the Principles. ZedX will investigate and attempt to resolve any complaints and disputes regarding use and disclosure of Personal Information in accordance with the Principles.

In compliance with the EU-US Privacy Shield Principles, ZedX commits to resolve complaints about your privacy and our collection or use of your personal information.

Questions, comments, or complaints regarding ZedX's EU-U.S. Privacy Shield Policy or data collection and processing practices can be mailed or emailed to ZedX at:

ZedX, Inc.

Attn: Chief Operating Officer

369 Rolling Ridge Drive

Bellefonte, PA 16823

information@zedxinc.com

ZedX has further committed to refer unresolved privacy complaints under the EU-US Privacy Shield Principles BBB EU PRIVACY SHIELD, a non-profit alternative dispute resolution provider located in the United States and operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbb.org/EU-privacy-shield/for-eu-consumers/ for more information and to file a complaint.

Please note that if your complaint is not resolved through these channels, under limited circumstances, a binding arbitration option may be available before a Privacy Shield Panel.

ZedX is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

1.6 Amendments

This privacy policy may be amended from time to time consistent with the requirements of the EU-U.S. Privacy Shield. We will post any revised policy on this website.

Revised August 16, 2016

2 ZedX General Policy

2.1 Introduction

The ZedX General Policy concerns the collection, use, retention, and security of personal information from users of ZedX products and services.

Users of ZedX products and services may elect to provide personal information via E-mail, online registration forms, or other mechanism applicable to the submission of content to a product. In addition, users may be required to provide ZedX with certain information in order to gain access to the products and services. This information is used internally, as appropriate, to handle the sender's requests and other matters pertaining to operation of a product. ZedX abides by the EU-U.S. Privacy Shield Principles regarding the protection of customer personal information.

ZedX products and services may also use this information to create summary statistics and to determine the level of interest in information available on a product to improve user interaction.

Some areas of the ZedX products and services may use a "cookie" temporarily stored in the visitor's computer memory (RAM) to allow the web server to log the pages you use within a product and to know if you have visited the product before.

Protecting your privacy is important to ZedX and our business partners and their affiliates. We want you to understand what information we collect and how it is used and shared with others. In order to provide users with a broad range of information and services as effectively and conveniently as possible, ZedX uses various technologies to manage information submitted to the products and services.

2.2 What Information Is Collected

ZedX may collect "nonpublic personal information" about you from the following sources:

- Information received from you regarding setup of your access to all products and services;
- Information about your transactions within a product while visiting the product with us, as well as transaction with our business partners; and
- Information we receive from third parties responsible for disseminating your information.

"Nonpublic personal information" is nonpublic information about you that we obtain in connection with providing services or information from the ZedX products and services to you and/or others. For example, nonpublic personal information includes information regarding your name, affiliation(s), location, history of data input or submissions, etc.

2.3 What Information We Disclose

We are permitted under law to disclose nonpublic personal information about you to other third parties in certain circumstances. For example, we may disclose nonpublic personal information about you to third parties to assist us in providing service or information to you (for instance, to a telecommunications provider), to government entities in response to subpoenas, to other organizations involved in the sharing of information from ZedX products and services, and to other service providers. We do not disclose any nonpublic personal information about you to anyone, except as permitted by law. Also, in the event we disclose nonpublic personal information about you, we disclose only so much as is required to provide the product or service requested, or to comply with authoritative governmental requests.

If you decide to stop using ZedX products and services, we will continue to adhere to the privacy policies and practices described in this notice.

2.4 Security Statement

ZedX also takes steps to safeguard information about users within a product. We restrict access to your personal information to those employees who need to know that information to provide information or services to you. We maintain physical, electronic, and procedural safeguards that comply with industry standards to guard your nonpublic personal information from unauthorized disclosure.

The internet service by which ZedX products and services are made available brings together a combination of industry-approved security technologies to protect data for ZedX and for the users of the products and services. It features user name and password-controlled system entry, Secure Sockets Layer (SSL) protocol for data encryption, and a firewall to regulate the inflow and outflow of server traffic.

2.5 Secure Data Transfer

To access the ZedX products and services, you may be required to use log-on procedures established by ZedX to begin a session of interaction with the products and services. Once the server session is established, the user and the server are in a secured environment. Data traveling between the user and the server is encrypted with Secure Sockets Layer (SSL) protocol. With SSL, data that travels between you and a product is encrypted and can only be decrypted with the public and private key pair (an industry standard). The server hosting a ZedX product issues a public key to the user's browser and creates a temporary private key. These two keys are the only combination possible for that session. When the session is complete, the keys expire and the whole process starts over when a user establishes another server session.

2.6 Firewall

Requests for data transmission to ZedX products and services must filter through a firewall before they are permitted to reach the server. A firewall blocks and directs traffic coming to the server. The configuration begins by disallowing ALL traffic and then opens holes only when necessary to process acceptable data requests, such as retrieving web pages or sending user requests for information or processing to the products and services.

Using the above technologies, ZedX attempts to make your interaction with the products and services as secure as possible.

Revised March 2, 2016

3 Privacy and Security Principles for Farm Data

3.1 Introduction

The Agriculture Technology Provider (ATP) Privacy and Security Principles for Farm Data concerns the collection, access, use, and security of farm data.

ZedX supports the following Agriculture Technology Provider (ATP) policies and principles for handling farm data.

3.2 Policies and Principles

3.2.1 Education

Grower education is valuable to ensure clarity between all parties and stakeholders. Grower organizations and industry should work to develop programs, which help to create educated customers who understand their rights and responsibilities. ATPs should strive to draft contracts using simple, easy to understand language.

3.2.2 Ownership

We believe farmers own information generated on their farming operations. However, it is the responsibility of the farmer to agree upon data use and sharing with the other stakeholders with an economic interest, such as the tenant, landowner, cooperative, owner of the precision agriculture system hardware, and/or ATP etc. The farmer contracting with the ATP is responsible for ensuring that only the data they own or have permission to use is included in the account with the ATP.

3.2.3 Collection, Access and Control

An ATP's collection, access, and use of farm data should be granted only with the affirmative and explicit consent of the farmer. This will be by contract agreements, whether signed or digital.

3.2.4 Notice

Farmers must be notified that their data is being collected and about how the farm data will be disclosed and used. This notice must be provided in an easily located and readily accessible format.

3.2.5 Transparency and Consistency

ATPs shall notify farmers about the purposes for which they collect and use farm data. They should provide information about how farmers can contact the ATP with any inquiries or complaints, the types of third parties to which they disclose the data and the choices the ATP offers for limiting its use and disclosure.

An ATP's principles, policies and practices should be transparent and fully consistent with the terms and conditions in their legal contracts. An ATP will not change the customer's contract without his or her agreement.

3.2.6 Choice

ATPs should explain the effects and abilities of a farmer's decision to opt in, opt out, or disable the availability of services and features offered by the ATP. If multiple options are offered, farmers should be able to choose some, all, or none of the options offered. ATPs should provide farmers with a clear understanding of what services and features may or may not be enabled when they make certain choices.

3.2.7 Portability

Within the context of the agreement and retention policy, farmers should be able to retrieve their data for storage or use in other systems, with the exception of the data that has been made anonymous or aggregated and is no longer specifically identifiable. Non-anonymized or non-aggregated data should be easy for farmers to receive their data back at their discretion.

3.2.8 Terms and Definitions

Farmers should know with whom they are contracting if the ATP contract involves sharing with third parties, partners, business partners, ATP partners, or affiliates. ATPs should clearly explain the following definitions in a consistent manner in all of their respective agreements: (1) farm data; (2) third party; (3) partner; (4) business partner; (5) ATP partners; (6) affiliate; (7) data account holder; (8) original customer data. If these definitions are not used, ATPs should define each alternative term in the contract and privacy policy. ATPs should strive to use clear language for their terms, conditions and agreements.

3.2.9 Disclosure, Use and Sale Limitation

An ATP will not sell and/or disclose non-aggregated farm data to a third party without first securing a legally binding commitment to be bound by the same terms and conditions as the ATP has with the farmer. Farmers must be notified if such a sale is going to take place and have the option to opt out or have their data removed prior to that sale. An ATP will not share or disclose original farm data with a third party in any manner that is inconsistent with the contract with the farmer. If the agreement with the third party is not the same as the agreement with the ATP, farmers must be presented with the third party's terms for agreement or rejection.

3.2.10 Data Retention and Availability

Each ATP should provide for the removal, secure destruction, and return of original farm data from the farmer's account upon the request of the farmer or after a pre-agreed period of time. The ATP should include a requirement that farmers have access to the data that an ATP holds during that data retention period. ATPs should document personally identifiable data retention and availability policies and disposal procedures, and specify requirements of data under policies and procedures.

3.2.11 Contract Termination

Farmers should be allowed to discontinue a service or halt the collection of data at any time subject to appropriate ongoing obligations. Procedures for termination of services should be clearly defined in the contract.

3.2.12 Unlawful or Anti-Competitive Activities

ATPs should not use the data for unlawful or anti-competitive activities, such as a prohibition on the use of farm data by the ATP to speculate in commodity markets.

3.2.13 Liability & Security Safeguards

The ATP should clearly define terms of liability. Farm data should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure. Polices for notification and response in the event of a breach should be established.

July 21, 2015