Data Protection Policy and Procedures

(Meets the GDPR European Union)

Compliance

All staff will be trained in handling personal data; what data is required for transactions and how to safely and properly store this data. Current staff will have ongoing training throughout the year and a yearly review of the policy and any changes that happened over the year.

Data program will be administered by our data protection officer and will oversee all processing. Officer will be responsible for a yearly assessment.

Privacy by design

We have established this data protection policy and procedures as a means of designing a program to manage and proactively protect our clients, potential clients, vendors, and stake holders' data and the resulting privacy.

We keep data protection as a key part of our IT systems, firewalls, and virus protection, and passwords.

Data protection will be a part of our policy and procedures in all areas of our business, and we will make corrections, and additions as new information and understanding become available.

Storing Data

The GDPR states that personal data cannot be stored outside of the EU and data is not to be transmitted back and forth between the EU. We cannot meet this requirement as we are located in the USA and we are required to collect certain bits of information that is submitted to US CBP as part of the Customs Clearance process. The minimum requirements will be requested. The normal processes of most shipments will not require us to request personal data but more company data.

Client and persons can redact information that is not required.

Documents that are personal in nature will be kept separate from file documents.

Documents with personal data will be kept in locked cabinets with restricted access.

All staff will have Security clearances in addition to ongoing training to safely handle personal data.

Privacy documents and personal data will be destroyed by means of a shredding.

Consent

Individuals can actively give consent and can redact other information that is not required.

We will advise what data we require to process the shipments, collect funds, pay funds and operate with the various U.S. Government agencies as required by law.

It must be understood that in most cases it is not our company that is requiring the data but is part of the requirements for export or import from or to the USA and failure to comply could result in storage or charges and they would be for the individual's account.

General company data that may be used for sales or marketing efforts will all have an-opt out and individuals have the ability to withdraw consent.

Breach Notification

Should a data breach happen we will notify the affected individuals. We will notify all agencies and will comply with all government agencies, as required. Further with incidents with affected individuals located in the EU, we will inform the Information Commissioner Office/ICO within 72 hours from the detection of the breach, as required by the GDPR.

We will advise and seek advice on how best to proceed to protect the individual's data from all relevant parties.

Right to Erasure

Individuals can request that their personal data be erased. Data electronically stored will be deleted as we are able, but we must remain in compliance with government regulations.

We will shred all personal data upon request of erasure.

Right to be informed

We will, upon request at the time of data collection, advise how we will be using the data and how it is submitted.

We will explain and provide the Government or agencies guidelines that require the data as requested.

In most cases that data is exchanged through EDI secured transmissions with CBP or other transport providers that exchange the data through the ACE system.

Right to Access

Individuals can obtain information from our company with how their data is being processed, and for what purpose, and where the data is being sent. We will make all efforts to respond timely; but will provide within 30 days from the request.

Right to data portability

We will, upon request in writing, make personal data available for the individual to be shared as they direct, as we are able.

We will not share data that will cost monies to transfer.

We will not share or forward data that our other security programs and procedures will not allow. We have TSA, CTPAT and other programs that require security and certain policies and procedures that also must be adhered to.

Right to restrict processing

We will, upon written request, restrict processing of individual data.

Further, we must restrict data processing if the individual advises their data is not accurate.

If the individual has objected to their data being processed. This will result possibly in the shipment not being handled by our firm and all charges as a result will be for the individual. Further we will invoice for outlays and for our time spent prior to being advised that they do not want their data processed. Restriction can be requested instead of erasure.

We will restrict the processing of the data but will store for future use as a legal claim.

We will also advise a third party of the individual's desire to have the restriction in place.

Right to object

Individuals have the right to object to their personal data being processed in the following ways:

Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling).

We will stop processing, unless we have compelling reasons or interests and are required as part of a claim or other legitimate process. We will advise if we are unable due to legal claims.

If any personal data is used for direct marketing we will immediately stop using the data upon notification by the individual.

We will stop using personal data for scientific/historical use upon notification of the data. This is not customary use of our data but is included to comply with possible uses no matter how infrequent.

Rights to related automated decision making and profiling

Under the GDPR, data processing may be characterized as “profiling” when it involves automated processing of personal data; and using that personal data to evaluate certain personal aspects relating to a natural person.

We do not use personal data in any automated decision-making process and we do not profile.

Goals

We are committed to safeguard all of our data and in particular the individual data we collect.

We will continue to seek out data experts and will seek their inclusion into our data protection policies and procedures.

We will train and monitor and assess our data protection procedures.

We will collect only the most basic of data and will safeguard and transmit to the industry and government guidelines.