Estate Valuations & Pricing Systems
Personally Identifiable Information Statement

Overview

EVP Systems offers four methods for evaluating historical securities for estate- and gift-tax purposes: EVP Office, EVP Everywhere, EVP Upload, and Professional Services.

No Personally Identifiable Information (PII) or Sensitive Personal Information (SPI) is required by any EVP Systems product or service, and such information is not transmitted to, or stored by, EVP Systems unless done so explicitly and intentionally by the client.

EVP Systems respects the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Infrastructure

All information that is transmitted to EVP Systems—personally sensitive or not—is, by default, sent using TLS 1.2, encrypted with a 2048-bit key. All information that is stored by EVP Systems is done so on filesystems and in databases encrypted using AES-128.

Off-site backups are performed nightly, transmitted using TLS 1.2 / 2048-bit key, and stored encrypted using AES-128.

EVP Office

EVP Office consists of four Windows desktop applications: EstateVal, GiftVal, CostBasis, and CapWatch. Each accepts information about a decedent or grantor (name, account number, notes, filename, etc.) for inclusion on the reports they produce. However, this information is never transmitted to EVP Systems, and remains local to the client's computer and filesystem, in EVP Portfolio files.

When the applications perform evaluations, they connect to the EVP Systems Data Center, but only send information required to make pricing queries: each security identifier in the portfolio (CUSIP, SEDOL, or ticker), the evaluation date (date of death, alternate date, date of gift, etc.), and the evaluation type. Even lot sizes are not transmitted.

Additional metadata for billing and auditing purposes—the client's account code, the user's Windows username, the EVP Administrator's username (if in use), the application's name and version, the machine's disk drive serial number—are sent. The Windows and EVP

Administrator's username delivery can be turned off, but will prevent ascribing specific evaluations to specific users during billing.

EVP Office offers an optional "Passthrough" feature which allows arbitrary information to be sent to the EVP Systems Data Center with each evaluation, and then returned to the client with the invoice details, allowing specific evaluations to be associated with specific passthroughs, at the client's discretion.

Passthrough data can be set to automatically mirror the portfolio's filename, the decedent's name, the portfolio account filed, or a combination of the decedent's name, the account, the evaluation date, and the report type; it can also be set to be an arbitrary text field on the application's main screen and is—by default—omitted entirely.

If Passthrough data is sent to EVP Systems, it is preserved in perpetuity as part of the accounting system. If a client requests its removal, EVP Systems will remove it completely as part of our GDPR and CCPA compliance.

EVP Everywhere

EVP Everywhere is webservice that offers similar functionality to EstateVal, but via a REST-based interface using JSON or XML. It is intended to be used by other software to run evaluations, rather than human beings.

EVP Everywhere has the same minimal data needs as EstateVal—the security identifier, the evaluation date, and the evaluation type—but also requires the size of each lot, since the calculations are done on the server-side instead of a desktop client. Accounting and auditing metadata sent consists of the client's account code. "Passthrough" data works the same as with EstateVal.

However, if full reports are required of EVP Everywhere, rather than raw data, the client will need to deliver every element that will appear on the report to EVP Systems with the request. This may include PII or SPI if that information is to also appear on the report. This information is fully optional and must be sent explicitly and intentionally by the client. If sent, it is stored (fully encrypted) in perpetuity by EVP Systems, but is subject to deletion at a client's request, per our GDPR and CCPA compliance.

EVP Upload

EVP Upload is a service that accepts file uploads, performs evaluations on them, and produces output that can include either inserting data back into the original file, producing traditional EstateVal reports, or both. It is intended to be a "file-based" or "batch" method for evaluations.

EVP Upload's data requirements are the same as EVP Everywhere—the security identifier, the evaluation date, the evaluation type, and the lot size. If full reports are to be produced, any PII or SPI that is to appear on them must also be sent, fully at the client's discretion. Account and auditing metadata consists of the client's account code. "Passthrough" data may be used but is not required. If sent, any proprietary information is stored (fully encrypted) in perpetuity by EVP Systems, but is subject to deletion at a client's request, per our GDPR and CCPA compliance.

Professional Services

Professional Services is a service provided by EVP Systems, to take the raw data for an evaluation sent by a client, enter it into the EVP Office applications, run the evaluation, and return the resulting reports to the client. It is intended for people too busy to run EVP Office evaluations for themselves.

As with EVP Everywhere and EVP Upload, the only information required by Professional Services to run evaluations is a list of the security identifiers, the evaluation date, the evaluation type, and the size of each lot. However, since reports are often being prepared for filing, PII and SPI are often included as part of the order: decedent's name, account numbers, notes, etc. Further, billing and auditing metadata include the client's account code and contact information, usually an e-mail address, but possibly also a phone or fax number.

Information sent to Professional Services is stored in encrypted EVP Portfolios files and on paper-printed copies kept in a locked filing cabinet in a locked office, protected by arm security. Electronic copies are kept in perpetuity and paper copies are purged via cross-cut shredding at Security Level 3 standards after three years. Both electronic and paper records are subject to client deletion requests via our GDPR and CCPA compliance.

Last updated: October 13, 2024