Veeva

eIDAS Compliance for CRM

Using Veeva CRM and Vault CRM for Compliant Signature Capture

August 2024

Why this guide?

Ensuring compliance with complex regulations like eIDAS is a critical challenge for life sciences companies. We understand that navigating these requirements can be time-consuming and complex. To help you streamline Veeva has developed this product guide to clarify how Veeva CRM and Vault CRM support eIDAS compliance for electronic signatures.

While Veeva's analysis indicates that our platforms can capture compliant signatures in the EU when properly configured to adhere to local regulations, we recognize that each organization has unique needs. This guide provides insights into how Veeva approaches eIDAS compliance and is provided for informational purposes only. It is essential to consider your specific business requirements and seek legal advice as needed.

Our goal is to empower you to make informed decisions about using Veeva's electronic signature features. By fostering collaboration between IT, operations, and compliance teams, we aim to simplify your journey to compliance. Veeva is committed to being your trusted partner in the life sciences industry, providing solutions that meet the evolving regulatory landscape.

Please don't hesitate to reach out if you have any questions or require further clarification. We're here to support your success.

Thank you,

Jenny Stohlmann, RAC
Senior Product Manager, CRM

Contents

What is “eIDAS”?

eIDAS is the prevailing electronic signature regulation in the EU. It covers a broad range of public and private activities, applying to people, businesses, and governments in all EU member states and certain service providers outside the EU.

At a high level, the regulation aims to create confidence across the EU that electronic signatures can be used securely and that relevant stakeholders will consider those signatures valid. Thanks to eIDAS, important agreements and transactions in the EU are not limited to paper.

Most importantly, eIDAS establishes a legal framework for electronic signatures and time stamps for those developing a sample program, including guidance around electronic documents, archiving, attestation of attributes, etc.

Is eIDAS a sampling regulation?

No. eIDAS is an electronic signature regulation, not a sampling regulation. Although stakeholders responsible for sample programs typically request eIDAS compliance, Veeva enables eIDAS compliance for all electronic signatures captured in CRM, including those for consents, medical inquiries, and contracts.

Why does eIDAS matter for sampling?

Electronic signature regulations like eIDAS matter to sampling programs when another law or regulation, known as a "predicate rule," requires sample documents to be signed. Suppose a predicate rule issued by a local regulator in the EU requires you to obtain a signature for sampling. In that case, you must comply with eIDAS if you use an electronic method to capture that signature.

What kinds of electronic signatures are there?

eIDAS specifically defines three types of electronic signatures. Depending on which type of signature is used, different requirements apply.

1. Electronic Signatures **(a.k.a. Standard Electronic Signatures):** data in electronic form that is attached to or logically associated with other data in electronic form and which is used by the signatory to sign
2. Advanced Electronic Signatures**:** an electronic signature which meets these four requirements:
    - It is uniquely linked to the signatory
    - It is capable of identifying the signatory
    - It is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control
    - It is linked to the data signed therewith in such a way that any subsequent change in the data is detectable
3. Qualified Electronic Signatures**:** an advanced electronic signature that is created by a qualified electronic signature creation device and which is based on a qualified certificate for electronic signatures

Our product design for Veeva and Vault CRM allows you to electronically capture and store handwritten signatures using a finger, stylus, or mouse on screen. In our sampling features, our design incorporates additional controls to comply with applicable regulations around the world that are specific to:

- Electronic signature capture
- Sampling life sciences products, including prescription and controlled substances.

Based on eIDAS definitions, Veeva and Vault CRM use Electronic Signatures

Why don't Veeva CRM and Vault CRM use Qualified Electronic Signatures for sampling?

eIDAS does not dictate the type of signature needed for any specific process. In fact, it establishes that an electronic signature cannot be denied legal effect based solely on the fact that it is in electronic form.

Would Qualified Electronic Signatures be "better," even if not required?

From a product design perspective, Qualified Electronic Signatures and Advanced Electronic Signatures would require an HCP to do pre-work to establish their digital identity (i.e., get an account) before signing. We do not think it is a good use of HCPs' time to set up accounts unless:

1. we offer them a functional benefit in return
2. there is a compelling business need, or
3. there is a compliance need.

We do not see these three reasons for sample signatures, so we keep it simple for HCPs.

What about Veeva's validation documentation?

Our sole focus is life sciences, and we always strive to keep our designs current with regulators' worldwide requirements.

Veeva has a computer system validation program that provides much of the documented evidence necessary for our customers to demonstrate that our software-as-a-service products can align with the regulatory context of use for sample signatures. In Compliance Docs, we provide information about the nature and scope of Veeva CRM and Vault CRM computer system validation to our customers. This documentation ranges from design verification infrastructure qualification to validation deliverables. Veeva composes its validation requirements for sampling features against applicable US electronic signature regulations and predicate rules. To ensure compliance worldwide, the validation team assesses whether the US requirements cover the ex-U.S. requirements.

An assessment of eIDAS Advanced Electronic Signature requirements vs. the US electronic signature regulation, 21 CFR Part 11, can be found in Compliance Docs. A table excerpt from Veeva's analysis can be found in the Appendix to this document. When reviewing, it is helpful to keep in mind that Veeva and Vault CRM use "handwritten signatures" as defined by US 21 CFR §11.3(b)(8):

> ***Handwritten signature*** *means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.*

What about the EU Digital Identity Wallet (EUDI)?

The idea of the EU Digital Identity (EUDI) was defined to address the need for secure digital authentication, and at this point, we do not believe it is relevant to sample requests.

EUDI regulations are still being revised. The first pilot programs for EUDI are ongoing, and we do not believe that sample signatures fit the early use cases for EUDI. While CRM enables validation of HCP licenses, it is uncommon for HCPs to be required to show identification when signing for samples. We may consider future innovation when the envisioned EEU Digital Single Market is closer to reality; CPs throughout the EEU can be expected to have obtained their EUDI during their education or credentialing process. Until then, we do not see the need to create an additional administrative barrier for an HCP to sign for samples.

Electronic Signatures and historical risk

Like handwritten signatures on paper, electronic signatures of all kinds are not immune from challenges in court or scrutiny during audits and inspections. A signee can always say, "I did not sign that," requiring more evidence. To our knowledge, however, this is a historically low-risk area for our industry. There are rarely serious disputes between companies that provide samples and HCP signees about the authenticity of a sample signature.

In the rare event that a sample fraud is believed to have occurred and is being investigated, a Standard Electronic Signature captured in a validated system like Veeva CRM or Vault CRM can provide significantly more information about when, where, and how the signature was created than paper (see Appendix). A Qualified Electronic Signature would not necessarily be accompanied by any more information to support such an investigation, and such matters are almost always resolved outside of a court.

Paper vs. electronic sample forms

Most recordkeeping is now done electronically, even for sample programs that still use paper forms. Veeva CRM and Vault CRM's ability to create timestamps and maintain audit trails for electronic records helps improve data integrity for electronic records from the start compared to paper forms converted to electronic archival records.

Starting with an electronically signed request also allows for more prompt inventory management and enforcing rules like sample limits. This reduces general risks of fraud, theft, and diversion that could lead to sample signatures being questioned. In some EU member states, sample limits are codified. The EFPIA Code of Practice also requires them. Minimizing oversampling in these states can help reduce the risk of investigations and disputes. Paper-based sample programs often try to enforce these rules after a sample has been disbursed. Compliance is comparatively easier with electronic signatures because enforcement can be done before signature capture.

Signature audits

While stamped signatures may not be easily detectible once a paper form has been scanned to an electronic archival record, a handwritten signature captured electronically provides the added benefit of visually comparing the signature on a specific record to another signature by the same signee.

The life sciences industry has conducted routine signature audit programs for years, including sending signature verification letters or emails to HCPs. These audit programs help the industry detect and investigate problems before they are found by regulators or escalated to a court. Compliance with eIDAS helps ensure that electronic signatures can be relied on. Veeva and Vault CRM facilitate signature audits with our View Signatures capability.

Summary

In the EU, sample program stakeholders are often aware of the eIDAS regulation. Still, they may need to learn how it applies to face-to-face, remote, or contactless electronic sample signatures captured in Veeva CRM and Vault CRM.

The Veeva product team believes our design meets all eIDAS requirements for Electronic Signatures and that signatures captured in Veeva CRM and Vault CRM are acceptable in courts in EU member states. We are unaware of local sample laws requiring Advanced Electronic Signatures or Qualified Electronic Signatures.

Our design relies on handwritten signatures that are not reusable by signees. This means that even though there is a historically low risk of fraud in sample programs that depend on electronic sample limits, inventory monitoring, and signature capture, our customers maintain the ability to perform signature audits and send signature verification letters that help identify potential fraud.

We believe our signature solutions provide appropriate security and traceability to investigate suspected fraud while limiting the need for HCP signees to perform administrative tasks like setting up an account or logging in before signing.

Appendix

Advanced Electronic Signature Requirements	Corresponding Part 11 Control
An Advanced electronic signature is a type of electronic signature which is required to meet certain specific requirements on signer identity, security, and sanctity of the signed document. The requirements specified under eIDAS are:	Definitions (§ 11.3): Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.
It is uniquely linked to the signatory.	11.10(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures in order to deter record and signature falsification 11.100(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. 11.100(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.
Is capable of identifying the signatory.	11.10(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. 11.200(a)(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. 11.300(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

Advanced Electronic Signature Requirements	Corresponding Part 11 Control
Is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control.	11.10(d) Limiting system access to authorized individuals 11.10(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.
Is linked to the data signed there with in such a way that any subsequent change in the data is detectable.	11.10(e) Use of secure, computer-generated, timestamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that is required for the subject electronic records and shall be available for agency review and copying. 11.50(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: 1. The printed name of the signer; 2. The date and time when the signature was executed; and 3. The meaning (such as review, approval, responsibility, or authorship) associated with the signature. 11.70 Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.