Castor CDMS | EDC and ePro 2025.x.x

21 CFR Part 11 & Annex 11 Assessment of Compliance

Document Version: 1.0

Table of Contents

Subpart A - General Provisions

The purpose of this document is to describe Castor CDMS | EDC compliance with the Food and Drug Administration's TITLE 21--FOOD AND DRUGS CHAPTER I--FOOD AND DRUG ADMINISTRATION, DEPARTMENT OF HEALTH AND HUMAN SERVICES, PART 11, ELECTRONIC RECORDS; ELECTRONIC SIGNATURES and EudraLex Annex 11: Computerised Systems

This document applies to Castor CDMS | EDC Version #2025.x.x as internally developed and tested. Castor CDMS | EDC has been designed and developed to be in compliance with 21 CFR Part 11, electronics records, electronic signatures and predicate rules when implemented and controlled effectively by the system User. Castor achieves compliance through a combination of risk assessment, SOP adherence, and by establishing a structured validated system. It is however the system User's responsibility to ensure that the software, as provided, is deployed and used in a manner that is compliant with 21 CFR Part 11 and Annex 11 requirements. The stem includes features such as Security controls through different access permissions, Audit Trails, Electronic Signatures with integrity checks.

Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to Agency inspection.

System Name:	Castor CDMS | EDC
System Version:	v2025.x.x
System Description:	Castor is a cloud-based clinical data management system solution, enabling researchers to easily capture and integrate data from any source. The Castor platform enables researchers to set up data capture forms, collaborate with colleagues, invite patients through questionnaires (ePRO) and import, export and analyze their data in a secure, compliant cloud environment, all without elaborate training or technical skills.

Definitions

Electronic Record – is any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system (refer to 21 CFR Part 11.3(b)(6)). Only records required by an agency regulation (FDA; Food, Drug & Cosmetic Act; or Public Health Services Act) to be maintained for inspection or to be submitted to an agency are considered within the scope of the 21 CFR 11 regulation. Note: a record is not considered to be "created" until it is committed to durable media.

Electronic Signature – is a digital representation 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 (refer to 21 CFR Part 11.3(b)(7)). For a signature to be considered an electronic signature under 21 CFR Part 11, it must be executed as the conscious action of the owner with a specific meaning (e.g., approval, release, review).

Computer System – is defined as a configuration of hardware components and associated software designed and assembled to perform a specific function or group of functions. Included in this definition are laboratory instruments, control systems, and computer systems, including hardware, software, peripheral devices, personnel, and documentation; e.g., manuals and Standard Operating Procedures. Third-party application software as well as internally developed application software is also included in this definition.

Regulation Reference – Reference to the specific paragraph in the 21 CFR Part 11 regulations and EudraLex Annex 11: Computerised Systems.

System Supplier - Castor system being assessed

System User- Castor's client, sponsor or CRO using the system being assessed.

Subpart B - Electronic Records

1.1 §11.10 Controls for Closed Systems

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and when appropriate the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

§11.10(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid altered records.

Annex 11:

1. Risk Management
3. Suppliers and Service Providers
4. Validation
10. Change and Configuration Management
11. Periodic Evaluation

System Supplier	System User
Castor validates each release per internal SOPs. The system and Quality Management System was developed using industry standard development tools, proper change control, and methodologies and was conforming to GxP requirements. Castor Suppliers undergo thorough assessments through SOP-SM-01 Supplier and purchasing procedure. Critical Suppliers undergo a Legal, Information Security, and Compliance evaluation. A risk based regulatory evaluation is made to determine if the supplier requires Validation/Qualification and/or Audit.	Users must assure themselves that System Supplier has validated the system based on requirements and guidelines when developing and testing the system. Pre-Qualification and requalification audits are available upon request based on internal procedures by contacting the Compliance department,

§11.10 (b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

Annex 11:

7. Data Storage
8. Printouts

System Supplier	System User
The system supports the ability to electronically display and print in human readable form all data contained within the system. 1.Printing options: - print empty CRF in PDF format: user can select the configurable elements that are to be printed out (helptext, additional info, calculation field templates, calc fields) - print surveys before or after data has been entered - print participant data in PDF format (individual & in bulk): user can select the configurable elements that are to be printed out (helptext, additional info, calculation field templates, hidden calc fields) 2. Export options - Export data in CSV, excel, SPSS, SAS, CDISC ODM OR zip file format: user can select the configurable elements that are to be printed out (comments, queries, verifications, encrypted fields) as well as choose display options in the printout (value or label) - choose how to export (tree, variable list, variables bulk) - choose which part of the Study to export (entire study of parts of it) - Export structure in XML format: user can choose to include annotations as well as choose which part of the Study to export (entire structure or parts of it)	Responsible for providing copies of records for inspection by the agency.

§11.10 (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

Annex 11:

6. Accuracy Checks
7. Data Storage
17. Archiving

System Supplier	System User
For Castor hosted solutions, all data is backed up routinely per established SOPs. Data backups are performed automatically throughout the day. The restore process is tested every 3 months. Castor also follows standards for record retention periods.	Client is responsible for maintaining all study related data and following their own retention policies.

§11.10 (d) Limiting system access to authorized individuals.

Annex 11:

12. Security

System Supplier	System User
Only authorized individuals are given access to specific clinical studies within Castor. Castor employs role-based user access based on a user's responsibilities within a specific clinical study. The system includes a login mechanism that requires each user to log in with a unique username and password to gain access to the system. Functions such as password requirements are supported by the system. The system servers are housed in a secure, access controlled environment. Only authorized personnel have access to the servers. Castor has SOPs on how to assign system access to authorized personnel.	Castor employs role-based user access based on a user's responsibilities within a specific clinical study when using the CDMS. The user is responsible for defining users and roles in the system. Should assign permissions based on role for access to different information within the system. Participant-facing ePRO functionality, made available to participants via email/URL, can have an access code system applied to prevent open access. This turned off/on as part of study configuration

§11.10 (e) Use of secure, computer-generated, time-stamped 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 required for the subject electronic records and shall be available for agency review and copying.

Annex 11:

9. Audit Trails
12. Security

System Supplier	System User
The system has a full audit trail. All information including reason for change (for clinical data changes), date, time, user, old value and new value is captured in the audit trail. The audit trail is retrievable throughout the record's retention period and is available to the agency for review, inspection and copy.	Responsible for ensuring the vendor maintains the data and associated audit trails retained and available.

§11.10 (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Annex 11:

5. Data
6. Accuracy Checks

System Supplier	System User
The system has been designed to allow the system User to configure workflows that guide the end user through the proper sequence of events. This configuration is possible at form level, for the user's role as well as at the level of data points (fields). Allowing access to various actions, parts, features or modules of the system can be easily managed by setting site level permissions per user or user role.	Responsible for configuring the system appropriately for thei intended use.

§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.

Annex 11:

5. Data
12. Security

System Supplier	System User
Only authorized individuals can access and use the system. Castor has been designed to require username and password to gain access. The application uses a role based security model to restrict data access only to authorized users. Study admins can add or remove other system users, as well as define permissions and roles. Access to individual parts of the system and or specific functionalities is determined by the level of permissions granted to each user, for each of the available study sites.	Responsible for configuring the system appropriately.

§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.

Annex 11:

4.Validation
5. Data

System Supplier	System User
Castor verifies source of access by the data stored after login in the API response (eg. login attempts, date & time, timezone for the user who is logged in). In addition, to confirm the integrity of the data that is being entered into the CRFs, any device/system used to enter data into our system (outside of keyboard and mouse being tested implicitly throughout the validation) such as a bar code reader, data integration would include some test (within the system directly leveraging the edit-checks) or outside the system through specific test steps (in API connection, error code returns success or failure for the entry)	Responsible for configuring the system appropriately. Responsible for validation of migration processes and ensuring data are not altered during migration processes.

§11.10 (i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

Annex 11:

2. Personnel

System Supplier	System User
Castor maintains CVs and JDs for staff that develop or maintain the system. They are hired based on education, training and/or experience, and properly trained according to Castor Policies and Procedures. Training records are maintained as per SOP.	It is the responsibility of the company deploying Castor for their clinical trial (e.g. Sponsor, CRO) to ensure that their employees developing, maintaining/administering and using the system have the appropriate training, education and experience. Similarly, the company deploying Castor retains responsibility to ensure participants are suitably trained in completion of any diaries or other patient reported outcomes.

§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.

Annex 11:

2. Personnel

System Supplier	System User
Castor requires users to accept Terms of Use when setting up a new user account for Castor.	Responsible for ensuring appropriate policies are in place and that compliance with those policies are monitored.

§11.10 (k) Use of appropriate controls over systems documentation including:

§11.10 (k) (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

Annex 11:

4. Validation
10. Change and Configuration Management
11. Periodic Evaluation

System Supplier	System User
System documentation can only be accessed by authorized individuals. Castor provides an online resource library and Castor Academy for users to have access to Manuals and User Guides with step-by-step instructions on how to get the most out of Castor systems.	Sponsors are responsible for the creation and maintenance o their own documentation that supports the operation and maintenance of the system.

§11.10 (k) (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Annex 11:

4. Validation
9. Audit Trails
10. Change and Configuration Management
11. Periodic Evaluation

System Supplier	System User
All documentation is electronically version controlled and any alteration is handled via change controls.	Responsible for the change control documents supporting their production environment.

1.2 §11.30 Controls for open systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10. as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity and confidentiality.

System Supplier	System User
Only authorized individuals can access and use the system. Castor CDMS | EDC has been designed to require username and password to gain access. The application uses a role based security model to restrict data access only to authorized users. The System includes a login mechanism that requires each user to log in with a unique username and password to gain access to the system.	Responsible for configuring the system appropriately. Castor CDMS | EDC employs role-based user access based on a user's responsibilities within a specific clinical study. The user is responsible for defining users and roles in the system. Should assign permissions based on role for access to different information within the system.

Functions such as password requirements are supported by the System. Single Sign-On: Study access can be accomplished using external Identity Provider credentials, allowing users to login to the system The System servers are housed in a secure, access controlled environment. Only authorized personnel have access to the servers. Castor has SOPs on how to assign system access to authorized personnel. Study access can be limited based on IP-range in addition to requiring mandatory two-factor authentication, at study and/or user level. In addition to our default encryption of data at rest and in transit, an extra application-level encryption layer can be enabled for sensitive data. This uses encryption keys managed off-site by a trusted third-party key management system. Within the application, fine-grained encryption and decryption authorizations can then be granted per study and site. Participant-facing surveys can be configured as part of study setup to require an access code on entry, sent to the participants' registered email address.	

1.3 §11.50 Signature Manifestation

§11.50 (a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

§11.50 (a) (1) The printed name of the signer; (2) The date and time when the signature was executed; (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

Annex 11:

14. Electronic Signatures

System Supplier	System User
Castor CDMS | EDC clearly indicates the full name of the signer, date and time of the signature(server-based in UTC) and the meaning/statement associated with the signature for each electronically assigned record. System users can configure the signature statement and configure which users can sign forms by assigning the required 'Sign' permissions to them. The information stored for each eSignature contains a Reference to username and full name.	Responsible for configuring the system appropriately.

§11.50 (b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

Annex 11:

14. Electronic Signatures

System Supplier	System User
This information is contained in the audit trail which is displayed in human readable format. This information is logged statically in the audit trail which is displayed in human readable format. The Audit Trail shows all changes that are made to a study, including changes both during building the form and during data entry. At the moment a system user cannot export the audit trail.However, Castor can export it upon request. The signature information is also displayed within the CRF every time a signature is applied to visit, form, a repeating data insurance or a participant record.	Responsible for configuring the system appropriately.

1.4 §11.70 Signature/record linking

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.

Annex 11:

14. Electronic Signatures

System Supplier	System User
All data is digitally signed using unique user's credentials. Electronic signatures within Castor CDMS | EDC are uniquely attributable to a single system user based on an individual's unique username and password. Castor CDMS| EDC clearly indicates the name of the signer, server date/time of the signature and the meaning associated with the signature for each electronically assigned participant record.	Responsible for configuring the system appropriately.

The information stored in the Audit trail is static, meaning that the event details cannot be modified or altered in any way, even after some information of the logged user (e.g. last name) are changed at a later point.	

Subpart C - Electronic Signatures

2.1 §11.100 General requirements

§11.100 (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

System Supplier	System User
Electronic signatures within Castor CDMS | EDC are uniquely attributable to a single system user based on an individual's unique username and Password. Once a signature is added by one individual, no additional ones can be added to the same element, nor can the signature be modified in any way. Audit trail events are created for signature - when applying digital signatures • when digital signatures are dropped /removed • when the signature statement is created • when the signature statement is changed	Responsible for configuring the system appropriately and enforcing appropriate policies to prevent reusing or reassigr a user's ID.

§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.

System Supplier	System User
Not applicable. System User's responsibility.	System User's responsibility to verify.

§11.100 (c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997 are intended to be the legally binding equivalent of traditional handwritten signatures.

§11.100 (c) (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

System Supplier	System User
Not applicable. This is the system User's responsibility.	Castor is not responsible for documenting the identity of system users. Responsibility for this task falls on the company deploying Castor for their clinical trial (e.g. Sponsor, CRO).

§11.100 (c) (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

System Supplier	System User
Not applicable. Castor is not responsible for this task. This responsibility falls on the company deploying Castor for their clinical trial (e.g. Sponsor, CRO)	Castor is not responsible for this task. This responsibility falls on the company deploying Castor for their clinical tria (e.g. Sponsor, CRO)

2.2 §11.200 Electronic signature components and control

Annex 11:

12. Security
14. Electronic Signatures

§11.200 (a) Electronic signatures that are not based upon biometrics shall:

§11.200 (a) (1) Employ at least two distinct identification components such as an identification code and password.

System Supplier	System User
When a user signs any form for the first time in a session after the login, the user is prompted to enter their "signing credentials" consisting of a username/email and password combination. Subsequent signings during the same session require one piece of information (i.e. password). This works per session, as described. After each session expires (i.e. log out, inactivity), the process is started over from the beginning.	Responsible for configuring the system appropriately.

§11.200 (a) (1) (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components: subsequent signings shall execute at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

System Supplier	System User
Castor CDMS | EDC requires two distinct identification components (User ID and password) during the first signing, and only one component (password) for all subsequent signings in the same system session.	Responsible for configuring the system appropriately.

§11.200 (a) (1) (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

System Supplier	System User
Castor CDMS | EDC requires two distinct identification components (User ID and password) for electronic signatures not performed in the same system session.	Responsible for configuring the system appropriately.

§11.200 (a) (2) Be used only by their genuine owners.

System Supplier	System User
This is covered in the Terms of Use agreed to by a user when initializing their Castor CDMS | EDC user account. Electronic signatures can only be used by the individuals with access to a specific study and that have the necessary permissions enabled/	Responsible for configuring the system appropriately and adopting and enforcing appropriate policies e.g. no username/password sharing. This is covered in the Terms of Use agreed to by a user when initializing their Castor user account.

§11.200 (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.

System Supplier	System User

Use of an individual's electronic signature would require collaboration of two or more individuals. Either the user would have to provide the password to another user, or the system administrator would have to collaborate with the user.	Responsible for adopting and enforcing appropriate policies.

§11.200 3 (b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

System Supplier	System User
N/A. Castor systems do not support the use of biometrics.	N/A

2.3 §11.300 Controls for identification codes/passwords

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

Annex 11:

11. Periodic evaluation

12. Security

§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.

System Supplier	System User
Each user has a unique user ID and password combination. The username cannot be used for more than 1 single account on each server that Castor provides. Castor CDMS | EDC is configured so that a strong password policy is enforced as well.	Responsible for configuring the system appropriately.

§11.300 (b) Ensuring that identification code and password issues are periodically checked, recalled, or revised (e.g. to cover such events as password aging).

System Supplier	System User
Each user has a unique user ID and password combination. The username cannot be used for more than 1 single account on each server that Castor provides.	Responsible for configuring the system appropriately and adopting and enforcing appropriate policies.

Castor CDMS | EDC is configured so that a strong password policy is enforced as well. Users are locked out of their account after 10 failed login attempts. Sessions automatically time out after 20 minutes of inactivity. Site/ Study administrators can enforce additional security policies, such as mandatory two-factor authentication or regular password rotation.	

§11.300 (c) Following loss management procedures to electronically de-authorize lost, stolen, missing or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable rigorous controls.

System Supplier	System User
Castor is responsible for the password policy for clients (product users). If Castor becomes aware that any credentials stored within our systems has been compromised, Castor can force (a subset of) users to reset their passwords and/or 2FA tokens in case of a compromise. Single sign on with federated identity management can be configured to align with customer's corporate password policies.	Responsible for configuring the system appropriately and adopting and enforcing appropriate policies.

§11.300 (d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

System Supplier	System User
The System can be configured to automatically lockout a user ID after a predetermined number of failed login attempts. At this time, the administrator can receive an immediate email alert. The number of failed attempts allowed can be adjusted by the administrator. The same functionality applies to electronic signature passwords. Users are locked out of their account after 10 failed login attempt (default). Only authorized study admins can proceed to unlock a locked account. Sessions automatically time out after 20 minutes of inactivity. Fine-grained access control is managed by the study administrato and authorizations are granted on a per person per site basis. All	Responsible for configuring the system appropriately and adopting and enforcing appropriate policies.

access is denied by default, preventing unauthorized access to data by other researchers or sites.	

§11.300 (e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

System Supplier	System User
Tokens or cards used to generate identification codes or passwords are not utilized by Castor. Castor products all follow the same SOP-DEV-01 Secure Development Procedure and SOP-QA-01 Validation Procedure which describe periodic reviews and evaluations.	Tokens or cards used to generate identification codes or passwords are not utilized by Castor.

Annex 11:

13. Incident Management

All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.

System Supplier	System User
Incident Management is tracked and assessed according to SOP-IS-02 Information Security Incident Management Procedure, SOP-SUP-01 Customer Support Procedure, and SOP-DEV-04 Service Incident Response Procedure. These procedures are followed by all products.	Responsible for establishing their own internal processes and procedures for handling incidents.

15. Batch release

When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.

System Supplier	System User
N/A	N/A

16. Business Continuity

For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.

System Supplier	System User
Business Continuity is implemented for the entire Castor organization according to POL-IS-02 Continuity Policy. External business continuity plans are managed via the Service Management Overview and tested annually via the IS-02-F01 Disaster Recovery Test Plan, whereas internal business continuity plans are managed via the IS-02-F03 Business Impact Analysis table.	N/A

Revision History

Document Version #	Description of Change	Author	Effective Date
1.0	Initial Release	Alexandra Marinescu	24-Mar-2025

Approval

The signatures below indicate approval of the content of this document.

Product Approval / Author	Signed by: Alexandra Marinescu Signer Name: Alexandra Marinescu Signing Reason: I am the author of this document Signing Time: 24-Mar-2025 | 4:57:40 PM CET 74108D50BFC84FAD8421FCED93143A12
Name and Title	Alexandra Marinescu Senior Product Owner
QA /Engineering Approval	Signed by: Eugenia Rudzenok Signer Name: Eugenia Rudzenok Signing Reason: I approve this document Signing Time: 24-Mar-2025 | 5:13:35 PM CET 618646CFF724461094DB6E70D3419B06
Name and Title	Eugenia Rudzenok QA lead
Compliance Approval	Signed by: Fatma Elfaghi Signer Name: Fatma Elfaghi Signing Reason: I approve this document Signing Time: 24-Mar-2025 | 1:05:37 PM EDT 06D97C1F835640F7923003BDA1E2E782
Name and Title	Fatma Elfaghi VP of Quality and Compliance

Certificate Of Completion

Envelope Id: 8A10F9ED-B29B-45CD-859D-C560EAD4CF73
Status: Completed
Subject: Castor CDMS_EDC and ePro 2025.x.x 21 CFR Part 11 & Annex 11 Assessment of Compliance
Source Envelope:
Document Pages: 21
Signatures: 3
Certificate Pages: 5
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Disabled
Time Zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Envelope Originator:
Alexandra Marinescu
Fred. Roeskestraat 115
Amsterdam, Amsterdam 1076 EE
alexandra.marinescu@castoredc.com
IP Address: 84.87.119.20

Record Tracking

Status: Original
3/24/2025 4:54:31 PM
Holder: Alexandra Marinescu
alexandra.marinescu@castoredc.com
Location: DocuSign

Signer Events	Signature	Timestamp
Alexandra Marinescu alexandra.marinescu@castoredc.com Sr.Product Owner Security Level: Email, Account Authentication (Required)	 Signature Adoption: Pre-selected Style Signature ID: 74108D50-BFC8-4FAD-8421-FCED93143A12 Using IP Address: 84.87.119.20 With Signing Authentication via Docusign password With Signing Reasons (on each tab): I am the author of this document	Sent: 3/24/2025 4:57:03 PM Viewed: 3/24/2025 4:57:36 PM Signed: 3/24/2025 4:58:03 PM
Electronic Record and Signature Disclosure: Accepted: 4/26/2021 1:36:52 PM ID: cade113c-ddd5-445e-a9fb-8aaefbb24109		
Eugenia Rudzenok yauheniya.rudzenok@castoredc.com QA Lead Security Level: Email, Account Authentication (Required)	 Signature Adoption: Pre-selected Style Signature ID: 618646CF-F724-4610-94DB-6E70D3419B06 Using IP Address: 82.74.247.61 With Signing Authentication via Docusign password With Signing Reasons (on each tab): I approve this document	Sent: 3/24/2025 4:58:06 PM Viewed: 3/24/2025 5:13:06 PM Signed: 3/24/2025 5:13:57 PM
Electronic Record and Signature Disclosure: Accepted: 6/21/2021 5:09:58 PM ID: f2f9e391-e833-436a-a758-0cf967b1255b		

Signer Events	Signature	Timestamp
Fatma Elfaghi fatma.elfaghi@castoredc.com VP Quality and Compliance Cewit B.V. – CFR Security Level: Email, Account Authentication (Required), Login with SSO	 Signature Adoption: Pre-selected Style Signature ID: 06D97C1F-8356-40F7-9230-03BDA1E2E782 Using IP Address: 174.61.72.147 With Signing Authentication via Docusign password With Signing Reasons (on each tab): I approve this document	Sent: 3/24/2025 5:14:00 PM Viewed: 3/24/2025 6:05:02 PM Signed: 3/24/2025 6:05:55 PM

Electronic Record and Signature Disclosure:
Not Offered via Docusign

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	3/24/2025 4:57:03 PM
Certified Delivered	Security Checked	3/24/2025 6:05:02 PM
Signing Complete	Security Checked	3/24/2025 6:05:55 PM
Completed	Security Checked	3/24/2025 6:05:55 PM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Ciwit B.V. – CFR (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Ciwit B.V. – CFR:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:
To contact us by email send messages to: compliance@castoredc.com

To advise Ciwit B.V. – CFR of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at compliance@castoredc.com and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from Ciwit B.V. – CFR

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to compliance@castoredc.com and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with Ciwit B.V. – CFR

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to compliance@castoredc.com and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Ciwit B.V. – CFR as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Ciwit B.V. – CFR during the course of your relationship with Ciwit B.V. – CFR.