FINAL DRAFT
International Standard

ISO/FDIS 32122

Transaction assurance in E-commerce — Guidance for offering online dispute resolution services

ISO/TC **321**

Secretariat: **SAC**

Voting begins on:
2024-12-12

Voting terminates on:
2025-02-06

Reference number
ISO/FDIS 32122:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 321, *Transaction assurance in E-commerce*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

E-commerce has drastically increased globally. Wide use of e-commerce has increased the number of related disputes, including cross-border ones.

At the time of dispute, traditional litigation or traditional in-person alternative dispute resolution (ADR) cannot substantially resolve the disputes, including cross-border ones. In other words, Transaction assurance in e-commerce cannot be achieved with traditional litigation or traditional in-person ADR, including for cross-border disputes. Online dispute resolution (ODR) has been gradually and widely used for e-commerce related disputes until now.

The safety and fairness of ODR are also important considerations, regardless if the ODR service was provided by an e-commerce operator or an outsourced ODR provider in order to be able to be used in a “real world setting”, including that it should not impose high costs, delays and burdens that are disproportionate to the economic value at stake. These are important factors in the assessment of a good e-commerce operator for all the stakeholders involved in e-commerce.

This document provides guidance for a safe, fair, accessible and effective ODR service. E-commerce operators can easily know what conditions are needed as a safe and fair ODR service, and thereby customers can find more e-commerce operators which provide the safe and fair ODR service.

This document has been developed with reference to available documentation relating to ODR service in e-commerce.

Transaction assurance in E-commerce — Guidance for offering online dispute resolution services

1 Scope

This document gives guidance on online dispute resolution (ODR) for e-commerce transactions including basic principles of ODR, technical recommendations and operational manuals to e-commerce operators (including e-commerce platform operators) which aim to develop their own ODR service and ODR providers that are outsourced by e-commerce operators.

NOTE This document is particularly useful for disputes arising out of cross-border, low-value e-commerce transactions. This document can apply to disputes arising out of both goods and service contracts.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 32110, *Transaction assurance in E-commerce — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 32110 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp
— IEC Electropedia: available at https://www.electropedia.org/

3.1
ODR provider
entity that administers and coordinates online dispute resolution (ODR) proceedings, including where appropriate, by administering an ODR platform

Note 1 to entry: An e-commerce operator or e-commerce platform operator can serve as an ODR provider.

3.2
ODR platform
online mechanism for generating, sending, receiving, storing, exchanging or otherwise processing communications.

3.3
ODR systems
entities involved in implementing, hosting or providing ODR services and platforms

Note 1 to entry: ODR systems can be provided by an ODR provider or an outsourced ODR systems vendor.

4 Basic principles

4.1 General

Online dispute resolution (ODR) is designed to promote confidence in e-commerce by providing quick electronic resolution and enforcement of disputes, including cross border ones. To achieve this objective, an ODR provider should adopt basic principles described in 4.2 to 4.10 when they plan, design, develop, implement, maintain and improve its ODR service.

NOTE Principles in this clause are based on the National Center for Technology and Dispute Resolution and International Council for Online Dispute Resolution Online Dispute Resolution Standards. [8]

4.2 Accessible

ODR should be easy for parties to find within a system and participate in and not limit their right to representation. ODR should be available in communication channels accessible to all the parties, minimize costs to participants, and be easily accessed by people with different types of abilities.

4.3 Accountable

ODR systems should be continuously accountable to the institutions, legal frameworks and communities that they serve. ODR platforms should be auditable and the audit made available to users. This should include human oversight of:

a) traceability of the originality of documents and of the path to outcome when artificial intelligence is employed;

b) determination of the relative control given to human and artificial decision-making strategies;

c) outcomes; and

d) the process of ensuring availability of outcomes to the parties.

4.4 Competent

ODR providers should have the relevant expertise in dispute resolution, legal, technical execution, language and culture required to deliver competent, effective services in their target areas. ODR services should be timely and use participant time efficiently.

4.5 Confidential

ODR providers should make every genuine and reasonable effort to maintain the confidentiality of party communications in line with policies that should be articulated to the parties regarding:

a) who will see what data;

b) how and to what purposes that data can be used;

c) how data will be stored;

d) if, how and when data will be destroyed or modified;

e) how disclosures of breaches will be communicated and the steps that will be taken to prevent reoccurrence.

4.6 Equal

ODR providers should treat all participants with respect and dignity. ODR should seek to enable often silenced or marginalized voices to be heard and strive to ensure that offline privileges and disadvantages are not replicated in the ODR process. ODR should provide access to process instructions, security, confidentiality,

and data control to all parties. ODR should strive to ensure on an on-going basis that no process or technology incorporated into ODR provides any party with a technological or informational advantage due to its use of ODR. Bias should be proactively avoided in all processes, contexts, and regarding party characteristics. ODR system design should include proactive efforts to prevent any artificial intelligence decision-making function from creating, replicating, or compounding bias in process or outcome. Human oversight should be required in ODR system design and auditing to identify bias, make findings transparent to ODR providers and users, and eliminate bias in ODR processes and outcomes.

4.7 Fair, impartial, and neutral

ODR should treat all parties equitably and with due process, without bias or benefits for or against individuals, groups, or entities. Conflicts of interest of providers, participants, and system administrators should be disclosed in advance of commencement of ODR services. The obligation to disclose such circumstances should be a continuing obligation throughout the ODR process.

4.8 Legal

ODR providers should abide by, uphold, and disclose to the parties relevant laws and regulations under which the process falls.

4.9 Secure

ODR providers should make every genuine and reasonable effort to ensure that ODR platforms are secure and data collected and communications between those engaged in ODR are not shared with any unauthorized parties. Disclosures of breaches should be communicated along with the steps taken to prevent reoccurrence.

4.10 Transparent

ODR providers should explicitly disclose in advance and in a meaningful and accessible manner:

a) the form and enforceability of dispute resolution processes and outcomes;

b) the risks, costs, including for whom, and benefits of participation.

Data in ODR should be gathered, managed, and presented in ways to ensure it is not misrepresented or out of context. The sources and methods used to gather any data that influences any decision made by artificial intelligence should be disclosed to all parties. ODR that uses artificial intelligence should publicly affirm compliance with jurisdictionally relevant legislation, regulations, or in their absence, guidelines on transparency and fairness of artificial intelligence systems. ODR should clearly disclose the role and magnitude of technology's influence on restricting or generating options and in final decisions or outcomes. Audits of ODR systems and platforms should identify metrics used to assess performance, making the accuracy and precision of these metrics known and accessible to any responsible entity and user. Users should be informed in a timely and accessible manner of any data breach and the steps taken to prevent reoccurrence.

5 Technical recommendations

5.1 General

The information obtained or generated through ODR process should follow the technical recommendations described in 5.2 to 5.6.

NOTE Technical recommendations in this clause are based on CRT (Civil Resolution Tribunal) Access to Information and Privacy Policies. [9]

5.2 Protecting personal information and privacy

Goal of providing transparent decision-making processes should be balanced with stakeholders' reasonable expectations that their personal information will not be disclosed, except where authorized and necessary to support the dispute resolution process. As a result, employees, members and contractors of an ODR provider have an obligation to protect personal information and only disclose it to third parties when required by legislation, the ODR provider's rules, a tribunal or court order, or where disclosure is necessary to satisfy the duty to act fairly and transparently.

To the extent reasonably possible, the ODR provider should:

— only include personal information, other than names, in notices, communications and decisions where there is an administrative justice or operational requirement to do so;

— take steps to ensure that any notices and communications that contain personal information are delivered to the address provided by the recipient for that type of communication and that notices and communications are not misdirected to incorrect destinations;

— avoid referring to personal information about non-parties, including names, in the decisions and orders, unless the personal information is required for administrative fairness or is a critical element in the decision; and

— where disclosure of personal information is authorized by the ODR providers' policy, only disclose as much personal information as is necessary to satisfy the request, the policy objectives, and the requirements of the ODR provider's rules.

If information is disclosed contrary to its policies, the ODR provider should immediately take steps to inform the proper recipients of the information and to remedy the inadvertent disclosure, and communicate to those whose data was breached the steps taken to prevent reoccurrence.

NOTE 1 ISO/IEC 27018 provides further guidance for protecting personally identifiable information in public clouds.

NOTE 2 ISO/IEC 27701 provides further guidance for privacy information management.

5.3 Anonymization of decisions

If a party establishes that the need for protection of personal information outweighs the goal of transparent proceedings, the human neutral should direct that a party's name and other personal information be removed, obscured, or anonymized in the decision. One way that this can be done is by using initials, instead of full legal names.

A neutral of the ODR provider can anonymize a decision on its own initiative or at the request of a party. If a party wants to ask the human neutral to anonymize a decision, it should make a request that the human neutral do so before the dispute enters either the mediation or decision making stage, or both.

In deciding whether to anonymize a decision, the human neutral should consider:

a) the circumstances of the case and nature of the evidence provided;

b) the potential impact of disclosure on the person; and

c) how anonymization would impact the goals of transparent decision-making processes and protection of personal information.

There are limitations to the human neutral and ODR provider's ability to anonymize a decision:

— The official version of the decision and copies of it provided to the parties should include party names.

— The ODR provider cannot anonymize a party's name in the version of an order that is validated for filing and enforcement in court.