International Standard

ISO 32122

First edition
2025-03

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

Assurance des transactions de commerce électronique — Recommandations pour les offres de services de résolution de litiges en ligne

Reference number
ISO 32122:2025(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 offering safe, fair, accessible and effective ODR services. 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
online dispute resolution 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 dispute resolution platform
online mechanism for generating, sending, receiving, storing, exchanging or otherwise processing communications

3.3
ODR system
online dispute resolution system
entity involved in implementing, hosting or providing online dispute resolution services and platforms

Note 1 to entry: An ODR system 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 Online Dispute Resolution Standards developed by the National Center for Technology and Dispute Resolution and International Council for Online Dispute Resolution. [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 the 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.

— If there are subsequent court proceedings about the decision, the human neutral or ODR provider, or both, can be obligated to file its records for the dispute with the court. This can include the full, unredacted version of the decision.

5.4 Records sealing

A human neutral or an ODR provider with human oversight, or both can, at any time, order that public access be limited for some or all information and records related to a specific dispute. Such an order or a direction can apply to records and information that would otherwise be available to the public or to a party to the dispute. The order or the direction can also include restrictions on which employees and members of the ODR provider can access the records and information.

Any order or any direction sealing the records for a dispute should specify the following:

a) the case number and style of cause for the dispute;

b) what types of records the order or the direction applies to;

c) who can have access to the records and what they can do with them (view only or replicate);

d) the reason for the order or the direction; and

e) the expiry date of the order or the direction, if any.

A request to seal records can be initiated by any person, whether or not that person is a party to a proceeding.

If there are subsequent court proceedings relating to the dispute, the human neutral or ODR provider, or both, can be required to file its records with the court. This can include any records affected by an order or a direction to seal them. As well, an order or direction to seal records does not prevent a party from submitting those records as part of the mediation or decision making process, or both. The order or the direction also cannot prevent a court or other tribunal from accepting those records as evidence in a proceeding with the court or other tribunal.

5.5 Security and storage of records

An ODR provider should protect personal information in its custody or under its control and ensure that personal information in its custody or under its control is securely stored.

Most information provided by parties during the dispute resolution process is recorded electronically in a storage of records. The storage is also used for generating records and sending them to the parties.

Parties to disputes can submit evidence and other information to the storage through their account. They are also able to use their account to view evidence and information submitted by other parties.

The storage should be subject to the highest possible levels of security. The accounts are password-protected and only provide access to designated dispute records stored in the storage.

An ODR provider can receive portable encrypted memory devices that contain electronic evidence files, e.g. if they are too large to transfer to the storage. In very rare cases, the ODR provider can accept physical evidence from a party. The human neutral or ODR provider, or both, should store these memory devices and physical records with secure methods (e.g. in a locked cabinet or in a secure file room).

The ODR provider should establish policies and procedures to support secure storage of records and to ensure those records and the information in them are only disclosed as per the technical conditions.

The ODR provider should ensure that its technological system(s), staff, members and authorized contractors:

a) maintain the integrity and security of its online systems, by:

— securing their authentication information for the systems and not sharing them with unauthorized users;

- viewing and downloading dispute records only where required for dispute resolution activities (e.g. by case managers for facilitation, by members for adjudication);
- using only secure methods (e.g. encrypted systems including memory devices) where it is necessary to download dispute information from the storage;

b) disclose records and information only where disclosure is required by the ODR provider or authorized by the technical conditions;

c) verify the accuracy of the intended recipient's address or contact information in each communication, before the communication is finalized and sent;

d) refrain from downloading electronic dispute records to a personal computer or electronic device, except where it is stored as a temporary record on the device in the course of viewing the record;

e) regularly (at least once per week) clear and delete the contents of download folders and temporary records caches or folders on computers or electronic devices that are used to access the systems or dispute records;

f) only print dispute records when clearly necessary and shred any printed copies as soon as the printed copy is no longer required;

g) ensure there is no ability for an unauthorized person or technological system to inadvertently access the contents of a record, including avoiding viewing records in public, unless absolutely necessary to do so;

h) store records on an encrypted memory device provided by the ODR provider where it is necessary to have a portable, electronic copy;

i) restrict access to the ODR provider's digital and physical records storage area to only those who have an operational need for access;

j) limit their disclosure and communication of dispute information or records to persons, technologies and circumstances authorized by the policies governing access to the records.

ODR providers have taken the following steps to ensure adherence to these security precautions and this policy, by:

- developing the storage functionality so that the system will in future generate and send most dispute communications, reducing the risk of technological and human error that results in a communication being sent to the wrong person;
- creating procedures, together with associated checklists, that reduce the potential for inadvertent unauthorized disclosure of information (e.g. a required step that artificial intelligence or staff, or both double-check contact information before sending correspondence);
- providing employees with privacy, security and records management training and audits of artificial intelligence processes regarding these issues tailored to the unique requirements of the ODR provider, as set out in this policy;
- requiring that employees and members acknowledge, in writing, that they have read and understood the applicable standards of conduct;
- sending regular communications to employees and holding regular meetings to remind them of the requirements of this policy and the need to maintain the security of the systems, physical records and oversee and analyse the audits undertaken regarding privacy, security and records management;
- where an inadvertent breach of a policy does occur, taking immediate steps to remedy it and conducting with the employee(s) involved a post-incident review, including of the relevant technology if artificial intelligence played a role in order to reduce the likelihood of future breaches and communicating to those whose data was breached the steps taken to prevent reoccurrence.

NOTE 1 ISO/IEC 27001 provides further guidance for establishing, implementing, maintaining, and continually improving an information security management system.

NOTE 2 ISO/IEC 27017 provides further guidance on information security controls for cloud services.

5.6 Access to records

An ODR provider should not disclose to the public personal information related to a minor or a party who has impaired capacity (a party with impaired capacity refers to a person who has a committee of estate, a representative appointed in a representation agreement, or an attorney appointed in an enduring power of attorney).

To support transparency in disputes involving minors or parties with impaired capacity, the ODR provider should have human oversight in determining whether, at its discretion, to provide access to dispute records, subject to the following:

— where the public would otherwise be entitled to access a dispute record, any information in the record that might identify a minor or a person with impaired capacity should be redacted or anonymized, if it is reasonably practical to do so (this also applies to a witness in the dispute);

— any system-generated indices of disputes that are made available to the public should include only the initials of minors, persons with impaired capacity or who are witnesses, instead of their full, legal names;

— in public versions of decisions and orders, the ODR provider should use initials to refer to persons who are minors, have impaired capacity or are witnesses, rather than their full legal names.

Staff and relevant artificial intelligence tools of the ODR provider responsible for reviewing draft decisions and orders should check to ensure any persons who are minors, have impaired capacity or are witnesses are referred to using their initials. The ODR provider can enter into agreements with other organizations and government agencies, authorizing the disclosure of dispute records to that other organization or government agency. The purpose of an information-sharing agreement should be to support:

a) a research project;

b) law enforcement or regulatory activities; or

c) any other purpose that is consistent with the ODR provider's mandate.

Where the ODR provider enters into an information-sharing agreement, the ODR provider will only disclose dispute records to the organization in line with the terms of the agreement. The terms of the agreement should:

a) restrict the further disclosure of the records outside the other organization in concurrence with this document; and

b) ensure the other organization takes steps to maintain the security of the records and prevent unauthorized disclosure of information, similar to those described in 5.5.

6 Operational manuals

6.1 General

E-commerce operators, including e-commerce platform operator, which try to develop their own ODR service, and ODR providers, that are outsourced by e-commerce operators, should establish their operational manuals based on the following provisions.

NOTE 1 Operational manuals consist of stages including: negotiation; mediation; and decision making stage. When a claimant submits a notice through the ODR platform to the ODR provider, the ODR provider informs the respondent of the existence of the claim and the claimant of the response. The first stage of proceedings — a technology-enabled negotiation — commences, in which the claimant and respondent negotiate directly with one another through the ODR platform. If that negotiation process fails (i.e. does not result in a settlement of the claim), the process moves to the second, mediation stage. In that stage of ODR proceedings, the ODR provider appoints a neutral, who communicates with the parties in an attempt to reach a settlement. If mediation fails, the third and final, decision making stage of ODR proceedings commences, in which case the neutral evaluates the dispute based on the information submitted by the parties and makes a decision for the dispute. Figure 1 illustrates ODR services flowchart.

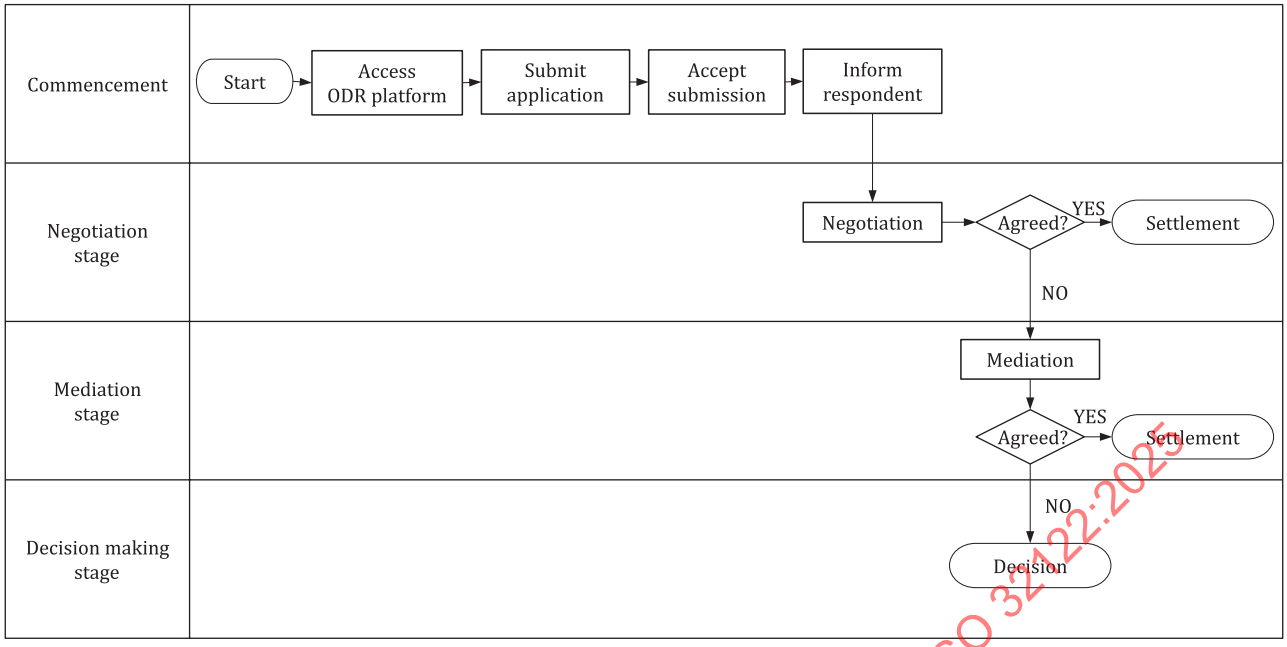

Figure 1 — ODR services flowchart

NOTE 2 The number of days for the administrative purpose can be changed as per the operation.

NOTE 3 Operational manuals in this clause are based on Model Procedural Rules for the APEC Collaborative Framework for ODR. [6]

6.2 Communications

a) All communications in the course of ODR proceedings should be communicated to the ODR provider via the ODR platform.

b) A communication should be deemed to have been received when, following communication to the ODR provider in line with a), the ODR provider notifies the parties of its availability, as per d).

c) The ODR provider should promptly acknowledge receipt of any communications by a party or the neutral at their electronic addresses.

d) The ODR provider should promptly notify a party or the neutral of the availability of any communication directed to that party or the neutral at the ODR platform.

e) The ODR provider should promptly notify all parties and the neutral of the conclusion of the negotiation stage of proceedings and the commencement of the mediation stage of proceedings; the expiry of the mediation stage of proceedings; and, if relevant, the commencement of the arbitration stage of proceedings.

6.3 Notice

a) The claimant should communicate to the ODR provider a notice as recommended in d). The notice should, as far as possible, be accompanied by all documents and other evidence relied upon by the claimant or contain references to them.

b) The ODR provider should promptly notify the respondent that the notice is available at the ODR platform.

c) ODR proceedings should be deemed to commence when, following communication to the ODR provider of the notice pursuant to a), the ODR provider notifies the parties of the availability of the commencement notice at the ODR platform.

d) The notice should include:

1) the name and designated electronic address of the claimant and of the claimant's representative (if any) authorized to act for the claimant in the ODR proceedings;

2) the name and electronic address of the respondent and of the respondent's representative (if any) known to the claimant;

3) the grounds on which the claim is made;

4) any solutions proposed to resolve the dispute;

5) the claimant's preferred language of proceedings;

6) the signature or other means of identification and authentication of the claimant or the claimant's representative, or both.

6.4 Response

a) The respondent should communicate to the ODR provider a response to the notice as recommended in b) within seven calendar days of being notified of the availability of the notice on the ODR platform. The response should, as far as possible, be accompanied by all documents and other evidence relied upon by the respondent or contain references to them.

b) The response should include:

1) the name and designated electronic address of the respondent and the respondent's representative (if any) authorized to act for the respondent in the ODR proceedings;

2) a response to the grounds on which the claim is made;

3) any solutions proposed to resolve the dispute;

4) the signature or other means of identification and authentication of the respondent or the respondent's representative, or both;

5) notice of any counterclaim containing the grounds on which the counterclaim is made.

c) The respondent can provide, at the time it submits its notice, any other relevant information, including information in support of its response, and also information in relation to the pursuit of other legal remedies.

6.5 Negotiation stage

a) If the response does not include a counterclaim, the negotiation stage should commence upon communication of the response to the ODR provider, and notification thereof to the claimant. If the response does include a counterclaim, the negotiation stage should commence upon communication of the response by the claimant to that counterclaim and notification thereof to the respondent, or after the expiration of the response period set out in 6.4, whichever is earlier.

b) The negotiation stage of proceedings should comprise negotiation between the parties via the ODR platform.

c) If the respondent does not communicate to the ODR provider by giving a response to the notice as recommended with the form contained in 6.4 b), within the time period set out in 6.4, a), or where one or both parties request that the process move to the mediation stage of the proceedings, or a party elects not to engage in the negotiation stage of proceedings, then the mediation stage of ODR proceedings should immediately commence.

d) If the parties have not settled their dispute by negotiation within ten calendar days of submission of the commencement of the negotiation stage of proceedings, the mediation stage of ODR proceedings should immediately commence.

e) The parties can agree to a one-time extension of the deadline for reaching settlement. However, no such extension should be for more than ten calendar days.

6.6 Mediation stage

a) Upon commencement of the mediation stage of ODR proceedings, the ODR provider should promptly appoint a neutral as recommended in 6.10 and should notify the parties:

   1) of that appointment as per 6.10 a), and;

   2) of the deadline for the expiry of the mediation stage under c).

b) Following appointment, the neutral should communicate with the parties to attempt to reach a settlement agreement.

c) If the parties have not settled their dispute by mediation within ten calendar days of being notified of the appointment of the neutral pursuant to 6.10 a) the ODR proceedings should move to the final (arbitration) stage of proceedings pursuant to 6.7.

6.7 Decision making stage

a) At the expiry of the mediation stage, the neutral should proceed to communicate a date to the parties for any final communications to be made. Such date should be not later than ten calendar days from the expiry of the mediation stage.

b) Each party should have the burden of proving the facts relied on to support its claim or defence.

c) The neutral should evaluate the dispute based on the information submitted by the parties and should render a decision. The ODR provider should communicate the decision to the parties and the decision should be recorded on the ODR platform.

d) The decision should be made in writing and signed by the neutral and should indicate the date on which it was made and the place of arbitration.

e) The recommendation in d) for:

   1) The decision to be in writing should be met where the information contained in the decision is accessible so as to be usable for subsequent reference; and

   2) The decision to be signed should be met where data is used to identify the neutral and to indicate his or her approval of the information contained in the decision.

f) The decision should state brief grounds upon which it is based.

g) The decision should be rendered promptly, preferably within ten calendar days from a specified point in proceedings as determined by the ODR provider.

h) A decision can be made public with the consent of all parties or where and to the extent disclosure is required of a party by legal duty, to protect or pursue a legal right or in relation to legal proceedings before a court or other competent authority.

i) The decision should be final and binding on the parties. The parties should carry out the decision without delay.

j) In all cases, the neutral should decide in accordance with the terms of the contract, taking into consideration any relevant facts and circumstances, and should take into account any usage of trade applicable to the transaction.

k) The neutral should apply the rules of law designated by the parties as applicable to the substance of the dispute. Failing such designation, the neutral should apply the law which is determined to be appropriate.

l) The neutral should decide as amiable compositeur or ex aequo et bono only if the parties have expressly authorized the neutral to do so.

6.8 Correction of decision

Within five calendar days after the receipt of the decision, a party, with notice to the other party, can request the neutral to correct in the decision any error in computation, any clerical or typographical error, or any error or omission of a similar nature. If the neutral considers that the request is justified, they should make the correction including a brief statement of reasons therefor within two calendar days of receipt of the request. Such corrections should be recorded on the ODR platform and should form part of the decision. The neutral can, within five calendar days after the communication of the decision, make such corrections on their own initiative.

6.9 Settlement

If settlement is reached at any stage of the ODR proceedings, the terms of such settlement should be recorded on the ODR platform, at which point, the ODR proceedings will automatically terminate.

6.10 Appointment of neutral

a) The ODR provider should appoint the neutral promptly following commencement of the mediation stage of proceedings. Upon appointment of the neutral, the ODR provider should promptly notify the parties of the name of the neutral and any other relevant or identifying information in relation to that neutral.

b) The neutral, by accepting appointment, should confirm that they can devote the time necessary to conduct the ODR proceedings diligently and efficiently.

c) The neutral should, at the time of accepting his or her appointment, declare his or her impartiality and independence. The neutral, from the time of his or her appointment and throughout the ODR proceedings, should without delay, disclose to the ODR provider, any circumstances likely to give rise to justifiable doubts as to his or her impartiality or independence. The ODR provider should promptly communicate such information to the parties.

d) Either party can object to the neutral's appointment within two calendar days:

   1) of the notification of appointment without giving reasons therefor; or

   2) of a fact or matter coming to its attention that is likely to give rise to justifiable doubts as to the impartiality or independence of the neutral, setting out the fact or matter giving rise to such doubts, at any time during the ODR proceedings.

e) Where a party objects to the appointment of a neutral under d) 1), that neutral should be automatically disqualified and another appointed in his or her place by the ODR provider. Each party should have a maximum of three challenges to the appointment of a neutral following each notice of appointment, following which the appointment of a neutral by the ODR provider should be final, subject to d) 2). Alternatively, if no challenges are made within two days of any notice of appointment, the appointment will become final, subject to d) 2).

f) Where a party objects to the appointment of a neutral under d) 2) above, the ODR provider should make a determination within three calendar days, regarding whether that neutral should be replaced.

g) Either party can object, within three calendar days of the final appointment of the neutral, to the provision by the ODR provider to the neutral of information generated during the negotiation stage. Following the expiration of this three-day period and in the absence of any objections, the ODR provider should convey the full set of existing information on the ODR platform to the neutral.

h) The number of neutrals should be one.