

INFORMAL COMMISSION GUIDANCE ON CONTINGENCY ARRANGEMENTS RELATING TO THE DECENTRALISED IT SYSTEM ESTABLISHED BY REGULATION (EU) 2023/1543¹

Last updated: 11 July 2026

Disclaimer: This Guidance has been prepared by the Commission services. It does not represent the official position of the European Commission and does not bind the Commission in any way.

Only the Court of Justice of the European Union is competent to authoritatively interpret EU law.

Regulation (EU) 2023/1543 (the “Regulation”) will apply from 18 August 2026. From that date, situations may arise in which communication through the decentralised IT system established by the Regulation is not possible, including where one or more relevant technical components are not yet operational. This Guidance addresses such situations only insofar as the Regulation is otherwise applicable and the relevant authorities and addressees can be identified and act in accordance with the Regulation.

This Guidance concerns the use of alternative means of transmission under Article 19(5) of the Regulation, focusing on situations in which the decentralised IT system cannot be used for the transmission concerned, whether due to persistent technical unavailability or a temporary incident. Any use of alternative means of transmission remains subject to the requirements laid down in Commission Implementing Regulation (EU) 2025/1550², in particular Section 3.3 thereof.

Pursuant to Article 19(5) of the Regulation, where communication through the decentralised IT system is not possible, the transmission shall be carried out by the most appropriate alternative means, taking into account the need to ensure an exchange of information which is **swift, secure and reliable, and allows the recipient to establish authenticity**. It should be noted that the Regulation remains otherwise applicable, and that any alternative means must comply with the other provisions of the Regulation, without modifying the workflows. Notably, the use of alternative means of transmission for an EPOC or EPOC-PR does not, in itself, alter the addressee, workflow or procedural safeguards provided for in the Regulation. Where the Regulation provides for direct transmission to the service provider, the use of alternative means should preserve that direct-transmission model, without prejudice to any notification, validation, review or enforcement mechanisms involving the enforcing authority where such involvement is required under the Regulation.

¹ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L 191, 28.7.2023, pp. 118).

² Commission Implementing Regulation (EU) 2025/1550 of 28 July 2025 establishing the technical specifications and other requirements for the decentralised IT system, referred to in Regulation (EU) 2023/1543 of the European Parliament and of the Council (OJ L, 2025/1550, 29.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1550/oj).

While Article 19(5) of the Regulation does not prescribe any specific alternative means of transmission, it does lay down a set of functional requirements that any such means must satisfy. The channel chosen must be the most appropriate and must be swift, secure, and reliable, while also enabling the recipient to establish the authenticity of the transmission. In practice, the most appropriate channel should be determined by reference to the concrete circumstances of the case, including technical interoperability, the nature, format and volume of the material to be transmitted, the level of security required, and considerations relating to speed, reliability and the recipient's ability to verify authenticity. Another factor to be considered may be whether there is an emergency case within the meaning of Article 3(18) of the Regulation. Cost and efficiency may also be considered, provided that they do not undermine those requirements.

In all cases, there must be an effective channel of communication between the issuing authority and the service provider - and, where applicable, the enforcing authority - satisfying the functional requirements laid down in Article 19(5) of the Regulation.

For greater clarity, physical delivery, such as personal delivery or courier delivery using traceable methods and proof of delivery, may be used where electronic transmission is not available or appropriate. Such means may allow the recipient to establish authenticity where they provide a documented chain of custody and reliable evidence of dispatch and receipt.

1) Preferred alternative means of transmission

On the basis of previous targeted consultations, the Commission services consider that the following alternative means of transmission are realistic and may be regarded as preferred options, where they are available, technically supported by the actors concerned and capable of satisfying the requirements of Article 19(5) of the Regulation and Commission Implementing Regulation (EU) 2025/1550. The list is neither exhaustive nor restrictive, and a combination of the means described below remains possible. For example, an EPOC may be transmitted via secure e-mail, while the requested electronic evidence is provided on a secure cloud server.

(a) Secure e-mail

Transmission of an EPOC or EPOC-PR may be carried out by secure e-mail using S/MIME or an equivalent mechanism ensuring encryption, sender authentication, integrity protection and, where possible, a signed or otherwise reliable acknowledgement of receipt. The e-mail address used for transmission should be an official, pre-validated address communicated by the issuing authority, enforcing authority or service provider, as applicable.

Similarly, electronic evidence may be transmitted by secure e-mail where the size and sensitivity of the material make this appropriate. In practice, however, e-mail attachment limits may make this channel unsuitable for larger evidence packages (there is no universal limit on e-mail attachments, but the usual limit is around 25 MB).

(b) Secure cloud solutions

The competent authorities of an issuing Member State may request that electronic evidence be uploaded to a secure government cloud storage service subject to strict access-control and authentication requirements. In such a case, the issuing authority should provide the service

provider with the technical and practical information necessary to enable the upload of the electronic evidence.

Alternatively, the authorities of a Member State may agree to retrieve the produced electronic evidence from secure cloud servers operated and managed by the service provider.

The application-layer protocol used for such exchanges should be technically supported by the provider of the secure cloud storage service, for example HTTPS-based object storage with multipart and resumable transfers, the SSH File Transfer Protocol (SFTP), or FTP over TLS (FTPS). Access means or credentials should be communicated through a separate secure channel.

The use of such alternative means should remain subject to confirmation that they enable the receiving authority to establish the authenticity and integrity of the transmitted material, for example by requiring the service provider to communicate, or otherwise make available, a hash digest of the e-evidence for the purposes of integrity verification.

(c) Use of secure platforms operated by service providers

This concerns the use of secure platforms operated by service providers for law enforcement requests, provided that such platforms can be used for the transmission of an EPOC or EPOC-PR, or for making electronic evidence produced pursuant to an EPOC available for download by the issuing authority, in a manner compatible with the Regulation.

It is recommended that each Member State establish objective criteria as to whether and how use of such platforms is acceptable – for instance, a Member State may require that each e-evidence package related to an EPOC is electronically signed by the service provider; similarly, a Member State could take into account trust stemming from the TLS certificate of the service exposed by the platform operated by the provider, together with other safeguards enabling the authenticity and integrity of the evidence package to be verified.

2) Other alternative means of transmission

The following alternative means of transmission have also been identified. While they could, in principle, be used, their identified limitations make them less viable in practice. They have therefore been retained for completeness but are not considered as “preferred” in the Commission services’ assessment.

- (a) Where available and possible, existing secure government networks for the purposes of communication between authorities and with service providers could be leveraged, insofar as they offer tangibly meaningful benefits compared to internet-based communication, without imposing disproportionate burden on service providers. The main challenge relates to the fact that such secure government networks are either not exposed to service providers or are not accessible cross-border from another Member State.
- (b) Qualified Electronic Registered Delivery Services (QERDS), within the meaning of Article 44 of the eIDAS Regulation, are capable of meeting requirements of speed, reliability and sender authentication, because they provide evidence relating to the handling of the transmitted data and require identification of the sender and the addressee. That said, QERDS do not automatically guarantee full technical

interoperability across all Member States, which remains dependent on the interoperability arrangements adopted between providers under the applicable standards framework. Moreover, the transmission capacity of QERDS is not fixed by eIDAS itself and is generally determined by the provider's technical policy, with practical limits commonly falling in a range of roughly 25 MB to 300 MB per message.

- (c) Certain ubiquitous secure messaging applications may, in exceptional circumstances, be useful for operational coordination and may, in principle, be capable of meeting some of the functional requirements set out in Article 19(5), notably relating to security and authenticity. Their use should nevertheless be assessed on a case-by-case basis, by reference to those requirements, and in principle their utility is limited when it comes to the transmission of large files.

The alternative means of transmission described above concern cases in which the competent authority proceeds under the e-evidence framework, but the decentralised IT system cannot be used for the transmission concerned. They should therefore be distinguished from cases in which the competent authority, for legal or practical reasons, decides not to use the e-evidence framework and instead relies on another applicable Union or international instrument, agreement or arrangement.

Alternatives to the e-evidence framework

Where the conditions of the Regulation are met, the use of the e-evidence framework should bring many advantages for seeking the production or preservation of electronic evidence. The e-evidence framework provides a standardised procedure under which an issuing authority may address an EPOC or EPOC-PR directly to the designated establishment or legal representative of the service provider, supported, where necessary, by the enforcement procedure laid down in the Regulation. In terms of speed, predictability and administrative effort, it will generally provide greater operational value than authority-to-authority or voluntary-cooperation channels.

However, the mechanisms established by Regulation (EU) 2023/1543 are not exclusive. Article 32(1) allows the use of other Union or international instruments, agreements and arrangements concerning the gathering of evidence falling within the scope of the Regulation. Where the e-evidence procedure cannot be operated effectively in the circumstances of a particular case, or another instrument is more appropriate for other specific reasons (e.g. different forms of evidence have to be collected from another Member State, which can be requested through one single European Investigation Order), the competent issuing authority may therefore consider another applicable avenue, subject to the conditions governing that avenue.

Annex I – Operational Decision Tree

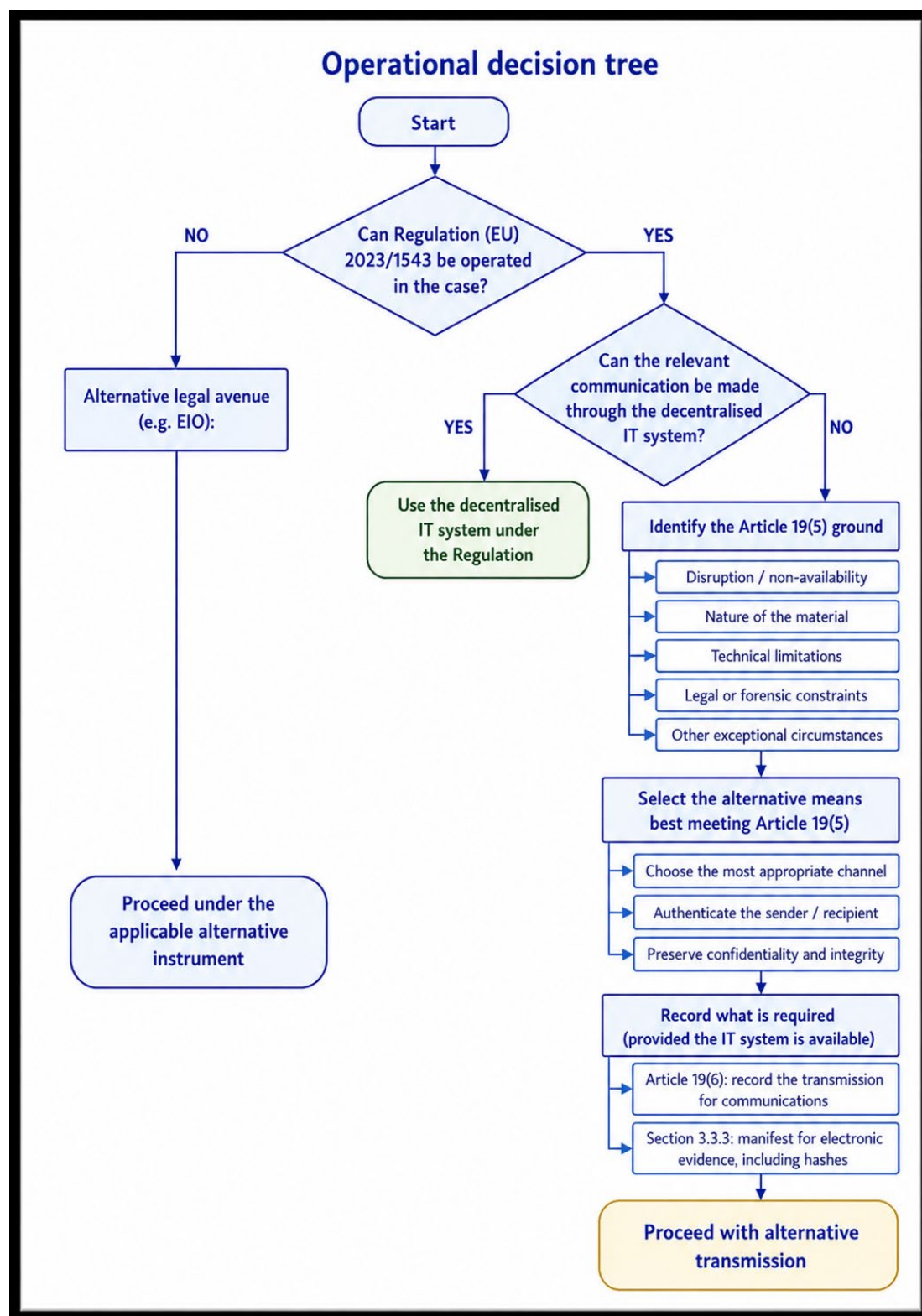


Figure 1: Decision Tree

Disclaimer: This diagram is intended solely to illustrate the decision-making process for identifying alternative legal avenues or means of transmission where Regulation (EU) 2023/1543 and/or the decentralised IT system cannot be used in a particular case. It is without

prejudice to Article 32(1) of Regulation (EU) 2023/1543, which remains applicable in any event.

** End of document **