The meeting was attended by representatives from all Member States (except for Greece), from Europol and Eurojust, members of the Council General Secretariat, a representative from the Counter-Terrorism Coordinator's office and an independent expert supporting the Commission. It took place in an open and constructive atmosphere, and many delegates contributed to the discussion, generating a large amount of helpful input for the ongoing reflection process.

The meeting focused on Strand 3 of the Council Conclusions: enforcement jurisdiction, notably on situations where Member States may use investigative measures in cross-border situations, either to compel an intermediary to produce evidence (production orders) or to directly access data stored remotely. A discussion paper with a number of specific questions was used to structure the debate.

The first part of the meeting focused on the definitions for types of data (subscriber, metadata and content data) and for service providers. Participants welcomed the idea of harmonized definitions and highlighted the need for a robust definition that could withstand the test of time and technical developments, but specific enough to encompass all necessary elements. Both communications data and data "at rest" needed to be included, and a suitable approach had to be identified for the overall scope especially when it comes to borderline situations (financial services provided online, online shopping sites). Participants mentioned problems in the distinction between electronic communications services, information society services and the online provision of services in other sectors in terms of information and data retention requirements. In that regard, although e-evidence requests can be addressed to electronic communication service providers (in the form of subscriber, metadata or content data) and ISS providers, equally the business models (and subsequently the data models) and the normative framework are different.

The participants then examined possible connecting factors permitting the direct use of an enforceable production order to a private party, as well as the effects of such production orders on other countries and ways to mitigate or address those effects. Notifying the affected Member State was identified as an option. In terms of possible connecting factors, Member States identified the headquarters of the company addressed, possibly in conjunction with its role as data controller; and a "business link" or provision of service to the issuing country as possible connecting factors for a reciprocal issuing and enforcing of production orders across and between Member States. For third country service providers, Member States discussed the option to mandate the presence of a representative in the Union, which could be addressed with production orders. In addition to issuing production orders, Member States also discussed the relevance of issuing preservation orders under these circumstances.
On the second day, Europol and Eurojust presented the recent Avalanche operation which highlighted some of the limits of existing legal frameworks while showing the beneficial effects of some forms of public-private partnership.

The participants then turned to situations of "loss of location", where it is unclear where the data is stored and hence which country might be affected by / the addressee of a cooperation request. Although some Member States appeared to assume that the data is always stored in its own country, others appeared to be more cautious and also considered the potential effect on other countries material. In this situation, a number of Member States permit direct access to data, subject to different safeguards. Participants discussed the necessary elements to establish loss of location, the investigatory measures permitted in different Member States, and the efforts required to identify the location. A time element was deemed relevant, which took the form of an "emergency" situation for some and was seen as less restrictive by others. Member States also highlighted differences in the extent to which they are able to take measures in the context of a loss of location situation, ranging from measures to identify location of data only to measures that safeguard the evidence remotely accessed by creating a local copy for prosecution purposes. There were also mentions of the possible impact of direct access on individuals' fundamental rights.

Afterwards DE presented a proposal for direct access from the device of a suspect or witness to remotely stored data in the context of an open search, where the remote system accessed is known to be in another Member State. Participants then engaged in a detailed discussion of the proposal's elements and its merits and disadvantages, notably on the notification of affected states, e.g. the state of the habitual residence of the person that the data relates to. Finally, they also considered the possibility of expanding it to cover other situations, notably where law enforcement remotely access data from a police computer or where the location of the data cannot be determined to be in a Member State.