Questionnary:

Having regard to the total number of requests mentioned under section 1.A.1.a:

1.A.2.a.3 how many (a) incoming and how many (b) outgoing transnational requests are processed by your country on an annual basis. When possible, please differentiate between judicial co-operation and non-judicial cooperation [Quantitative Reply]

According to information from National Criminal Investigation Service (KRIPOS), either incoming nor outgoing requests per year are being numbered. However, KRIPOS underlines the significance of traffic data in inquiries of serious crimes. The number of requests from Norway to cooperating police authorities is therefore significant, and it is reasonable to suggest that there are at least 1.000 request each year. The number of requests to Norway (incoming requests) is also significant, however lower than outgoing requests.

1.A.2.a.4 what is the ratio between national and transnational requests (total number of transnational requests)? [Quantitative Reply]

According to 1a2a3, no secure statistics exists. The number of incoming requests is suggested to be lower, than outgoing requests.

1.A.2.c Which authority takes the decision in your country to issue a transnational request? Are all law enforcement authorities entitled to make or prompt to make a transnational request?

Which authority that issue an outgoing request depends of what regulation that is being applied. According to the Nordic Convention on information exchange (1974), the request can be issued directly from a Nordic police district to another Nordic police district. Requests to other European countries are issued according to the 1959 Convention, or the Schengen Convention. These requests are mainly issued on a public prosecutor level.

1.A.2.d Does your country have a central point that issues outgoing requests or receives incoming requests? If so, please provide details about these central points.

Normally, incoming and outgoing requests are being forwarded through Interpol. However, in ongoing inquiries there is often established directly contact between the investigators in different countries, and Interpol is therefore not used in these inquiries.
Supplying questions from the European Commission after meeting Dec. 14th:

1) The Norwegian Criminal Procedure Act, § 215 a ("freezing provision"): Unfortunately, there is no statistics on use of this provision. According to information from Kripos, the § 215 a provision has been used only once the last years by Kripos. There is no information on use in other police districts. However, search in the electronic case-law database ("Lovdata") on this provision has no hits, unless one decision from the High Court, where the provision is mentioned. Therefore, there is an understanding that the § 215a provision very seldom has been used. The main reason for the non-use of the provision seems to be that the Norwegian Telecommunication Authority normally grants access to traffic data within rather short time. When the police requests data within short intervals by requesting the Norwegian Telecommunication Authority according to the telecommunication act, the freezing procedure according to the Norwegian Criminal Procedure Act § 215 a is not necessary. Both Telenor and NetCom – the largest telecommunication companies in Norway – confirms this understanding. Neither of the companies numbers § 215a-requests. However, NetCom suggests that annual average of requests normally don’t exceed 5.

2) Police access to identifying “anonymous” pre-paid phone cards (according to the telecommunications act): According to Kripos, there is no statistics on the number of searches on pre-paid phone cards. Our representative in Kripos informs that the number of searches being done each year securely is “more than several thousands”.

Law enforcement issues re. Data Retention Directive

1. Providers do not keep a register for designated IMEI numbers. Providers with access to electronic communications networks can however, via the phone’s IMEI number identify which SIM cards that have been used in the relevant hand set (mobile phone). The providers keep a register including information re. who/which legal entity is the rightful user of the phone number(s). The user name will also be registered with the provider. The provider is according to the ecom regulations obliged to keep (and store) information re. end users connected to a subscription, see pt. 5 below.

2. The providers are entitled to submit information mentioned above in pt. 1 to the prosecuting authority or the police despite the providers’ obligation to maintain secrecy of the content of electronic communications, according to the Electronic Communications Act (Act No. 83 of 4 July 2003), Section 2-9, third paragraph.

3. IMEI numbers are accessible from the providers due to technical reasons. Phone centrals for mobile services which switch these communications ask the so-called EIR register, which is the central data base holding information re. approved mobile phones, as to whether the relevant IMEI number is approved for use within this network.

4. Information about IMEI numbers and which SIM cards that can be connected to a hand set has proven useful in investigation and prosecution of criminal conduct. IMEI numbers are also important for the police in order to identify relevant phone numbers related to communications control.

5. In Norway pre-paid phone subscriptions and other phone service subscriptions are regulated identically. This implies that the operators’ duties according to present regulations are applicable also to pre-paid subscriptions, including the possibility for identification of the end users. Regulations as follows:

- The Ecom Regulations Section 6-2 demands unique registration of all end-users (“enabling the clear identification of those registered”). An account of information about end-users shall enable unambiguous identification of those registered, as well as enabling the geographical locating in connection with emergency calls. Personal identification numbers and organizational numbers can serve as such indicators.
- The request for unique identification in Section 6-2 is enforced quite rigidly by the NRA (Post- og teletilsynet). Amongst other reasons it is necessary to serve the police’s need for sufficient and adequate information, in order to start communication control procedures (cf. The Penal Act Chapter 16 a). Furthermore, it serves as a hindrance for illegal establishing of mobile subscription by ID theft. The NRA’s practice regarding pre-paid subscription cards (“cash cards”) was intensified approximately five years ago.
- The NRA has successively specified the obligation in Section 6-2, including the fact that the service should not be activated until the end-user is uniquely identified. The NRA consider the practice below as a satisfactorily way of meeting this demand:
  ✓ Persons registered in the directory of residents: The provider checks if information given by the customer is identical with information in the
directory of residents. Furthermore, the provider is obliged to send an order confirmation to the customer’s address as registered in this directory.

✔️ Persons not registered in the directory of residents: These customers must provide identity information at the purchase. Identification demanded will normally be passports or other sufficient identity documents, such as banker’s card Norway Post identity card etc.

- Establishing of a pre-paid subscription normally takes place like this: Start-up kits are bought at the providers’ premises. When the SIM-card is placed in the hand set (the mobile phone), the first call is routed to Customer Services (a routine established when the NRA intensified their practice regarding registration of pre-paid cards’ customers). The customer is obliged to give relevant personal information, and if this matches the directory of residents’ information, the service will be activated. The provider sends a written order confirmation to the customer’s address according to the directory of residents. Customers not listed in this directory must produce written documentation as listed above when making the purchase at the provider’s.

- The providers’ cost regarding the obligation to register is not deemed to be disproportionate. The NRA has not received any comments from the providers regarding too high implementing costs of these provisions.

- The Electronic Communications Act and Regulations have no conditions regarding consequences of non-use of pre-paid cards. However, the providers often have agreement clauses implying cancelling after a certain amount of time, provided the subscription is inactive. For instance, Telenor’s agreements contain a condition of 15 months’ validity after the last charging of the pre-paid card. After 15 months the customers have a 2 months’ time limit to recharge the account. If this doesn’t happen, the subscription will be terminated and a new start-up kit will have to be purchased.

---

1 IMEI numbers: International Mobile Equipment Identifier. All mobile phones have a unique IMEI number. The number is controlled against the provider’s IMEI register every time the phone is activated.