



Council of the
European Union

Brussels, 7 November 2016
(OR. en)

14001/16

JAI 899
COSI 180
DAPIX 197
ENFOPOL 397
COPEN 320
CYBER 125
FREMP 176
TELECOM 215

COVER NOTE

From: Dr de Maisière, MdB, Minister of Interior of the Federal Republic of Germany
and
Mr Bernard Cazeneuve, Minister of Interior of the French Republic

date of receipt: 4 November 2016

To: Mr Robert Kalinak, Council Presidency, Deputy Prime Minister and Minister of the Interior of the Slovak Republic

Subject: German-French letter concerning cooperation between law enforcement agencies and electronic communication service providers

Delegations will find attached document from Dr de Maisière and Mr Cazeneuve to Mr Robert Kalinak.



Bundesministerium
des Innern



MINISTÈRE DE L'INTÉRIEUR

Mr Frans Timmermans
First Vice-President of the
European Commission
Rue de la Loi 200/Berl 12/78
1049 Bruxelles/Brussels
BELGIUM

Mr Dimitris Avramopoulos
Commissioner for
Migration, Home Affairs and Citizenship
European Commission
Rue de la Loi 200/Wetstraat 200
1049 Bruxelles/Brussels
BELGIUM

Mr Julian King
Commissioner for Security Union
European Commission
Rue de la Loi 200/Wetstraat 200
1049 Bruxelles/Brussels
BELGIUM

Mr Günther Oettinger
Commissioner for
Digital Economy and Society
European Commission
Rue de la Loi 200/Wetstraat 200
1049 Bruxelles/Brussels
BELGIUM

Mr Andrus Ansip
Vice-President
Commissioner for
Digital Single Market
European Commission
Rue de la Loi 200/Wetstraat 200
1049 Bruxelles/Brussels
BELGIUM

Ms Vera Jourová
Commissioner for
Justice, Consumers and Gender Equality
European Commission
Rue de la Loi 200/Wetstraat 200
1049 Bruxelles/Brussels
BELGIUM

Dr. Thomas de Maizière, MdB
Bundesminister

POSTANSCHRIFT
Alt-Moabit 140, 10557 Berlin

Bernard Cazeneuve
Ministre de l'Intérieur

POSTANSCHRIFT
Place Beauvau, 75008 Paris

Berlin, 28 October 2016

CC

Council Presidency
Deputy Prime Minister and Minister of the Interior
of the Slovak Republic
Mr Robert Kaliňák
Rue de la Loi 175/Wetstraat 175
1048 Bruxelles/Brussels
BELGIUM

Secretary-General of the
Council of the European Union
Mr Jeppe Tranholm-Mikkelsen
Rue de la Loi/Wetstraat 175
1048 BRUXELLES
BELGIEN

Counter-Terrorism Coordinator
Mr Gilles de Kerchove
Rue de la Loi/Wetstraat 175
1048 BRUXELLES
BELGIEN

Dear Mr Vice President, dear Commissioners,

The recent terrorist attacks committed in Europe's Member States and the ongoing investigations into recent failed attempts, have underscored the decisive role that electronic communications play in the preparation and execution of these acts. Hate speeches, calls for violence and exchanges linked to the glorification of terrorism or planned terrorist attacks are widely published via the multitude of applications that are used each day by the general public.

These different tools pose practical and legal difficulties for investigators and judicial authorities alike in that they allow for the free exchange of fully encoded messages to anyone who has access to these services. Not only are these messages often automatically deleted after a certain period of time, but conversation groups or chat rooms can include thousands of participants. Today, competent authorities can face insurmountable obstacles when they request the technical assistance of service providers in analysing the data of messages sent by suspects.

As we stated in the joint letter of 23 August 2016 addressed to the European Commission, solutions that allow for effective investigation into encoded data linked to potential terrorist attacks or organised crime are vital. Of course, it is just as indispensable to protect an individual's right to digital freedom by ensuring the

availability of highly secure encrypted systems and by respecting the principles of proportionality and necessity that are inherent to our fundamental rights and the notion of law-abiding States. Encryption technologies are a key factor in the security of and trust in Europe's digital ecosystem and their reliability must be safeguarded at all costs.

At a time where our citizens are confronted with the constant threat of a terrorist attack, we owe it to them to meet this challenge, and that means achieving the following objectives:

- Being able to rely more on the **responsibility of electronic communication service providers, particularly those that are not based within the Union:**

Our ability to apprehend these operators, notably those that are not governed by a stable administration within the European Union, is critical. Member States must be able to count on the collaboration of representatives of operators when it comes to criminal investigations.

The establishment of genuine links between legal authorities and service providers must become the norm. Given the stakes involved, each service provider must have a point of contact who is able to directly respond to legal requisitions from the competent authorities of Member States.

- Reinforcing the **legal obligation of electronic communication service providers to cooperate** with the competent authorities of Member States when it comes to criminal investigations:

All too often, Member State authorities are faced with a refusal by service providers to provide information on legal grounds that we must be able to override.

Electronic communication service providers must be able to contribute more to the successful outcome of investigations by being authorised to provide data linked to users or connections; in addition, data for European customers must be stored in a jurisdiction where direct cooperation with competent authorities of Member States is authorized.

- Ensuring greater speed and **reactivity in the processing of requisitions by judicial authorities** in order to obtain information from electronic communication service providers;

- improving the extraction of content that may be linked to terrorism:

Cooperation between law enforcement agencies and electronic communication service providers must also allow for the immediate and permanent removal of public messages promoting terrorism. Where this is not possible, recourse to the EU-IRU of Europol could be recommended in addition to national measures.

These objectives must guide the discussions and work of Member States and the Commission in the coming months in order to define normative, operational, pragmatic and efficient solutions to the issue of encryption in investigations linked to terrorism. Their work must also guarantee the respect of individual freedoms.

In order to share our concerns and in line with the topics raised during the JHA Council meeting in June 2016, we request that the issue be included in the agenda of the JHA Council meeting of 18 November 2016.

Yours sincerely



Dr. Thomas de Maizière, MdB
Bundesminister des Innern

Bernard Cazeneuve
Ministre de l'Intérieur