FEDERAL POLICE

General directorate of judicial police (DGJ)
Directorate special units (DSU)
National Technical & Tactical Support Unit (NTSU)
Central Technical Interception Facility (CTIF)

Avenue de la Cavalerie 2
1040 Bruxelles
Tel.: +32 (0)2 642 77 11
Fax: +32 (0)2 642 77 10
E-mail: dsu.ntsu.ctif.perm@police.belgium.eu

Legal obligations to cooperate for network operators and providers of electronic communications services

General information about the legal framework, obligations, remuneration and TANK cooperation platform for the exchange of information between the parties involved

SUBJECT:	**Information brochure**
RECIPIENTS:	**Network operators** **Providers of electronic communications services**
FILE MANAGER:	Luc Beirens Tel. +32 2 642 76 48

DOCUMENT TYPE:	**INFORMATION BROCHURE**	CLASSIFICATION:	**-**
REFERENCE:	**DSU/NTSU/264/2017**	PAGES:	**23**
PUBLICATION DATE:	**17/05/2017**	ATTACHMENTS:	**-**
CONFIDENTIALITY:	**PUBLIC**	REF PC:	**-**

Police

Legal obligations to cooperate for network operators and providers of electronic communications services

General information about legal framework, obligations, remuneration and TANK cooperation platform for the exchange of information between parties involved

Table of contents

1 General introduction on the obligation of cooperation

In today's society, where almost everybody uses electronic means of communication and computer systems, it is a necessity for the different authorities to be able to investigate in this "virtual" environment in order to respect the rights of society and citizens and furthermore to detect, identify, and locate suspects and if necessary, obtain or intercept information about their communications.

It is clear that these investigations are not possible without the cooperation of network operators or providers of electronic communications services (hereinafter referred to as "operator" and "service provider").

To this end, the legislature has granted various powers to certain judicial authorities and intelligence services and, on the other hand, imposed various obligations on operators and service providers.

In implementing the statutory provisions, various authorities are involved in formulating this cooperation between governments and operators and service providers. The government strives to make this cooperation as efficient and economical as possible.

For these reasons, the Federal Police's NTSU CTIF Service was identified as a competent intermediary for the exchange of questions and answers between the authorities and operators and service providers for a number of forms of cooperation.

An exchange platform called TANK is currently being developed to automate the data exchange. In the future, connecting to this platform will be a prerequisite for both operators and service providers to be compensated by the government for the co-operation provided. Currently the legal framework requires that operators are obliged to use this platform as soon as it becomes available.

This document aims to provide a brief overview of the legal framework, the powers, the possible requests for assistance, the obligations of operators, penalties, the role of the various authorities, the TANK project, and the demand for engagement as an operator or service provider.

This document does not have the pretence to be complete at all. It is an incentive for anyone who needs to acquire knowledge about cooperation between the government, operators and service providers.

We hope this document may improve cooperation between stakeholders.

Luc Beirens
Head of CTIF

2 Legal framework

2.1 Introduction

The legal framework within which an operator of a network or the electronic communications service provider is held to work with the government is formed by a series of articles spread across various Acts and Royal Decrees (RD).

Below you will find an overview of the most important articles in these Acts and Royal Decrees with a brief description of the content and the competent government that may request this cooperation. An in-depth reading of these articles is necessary for operators and service providers to be able to estimate their full scope.

This overview is also limited to cooperation with judicial authorities and intelligence services. Other authorities also have powers to question operators and service providers, but this document does not go further in detail regarding these authorities.

2.2 Basic provisions: respect for privacy and secrecy of communications

The personal and family life of each person is guaranteed by Article 22 of the Constitution and Article 8 of the ECHR (European Convention on Human Rights). Any deviation from this is possible only on the basis of a law. According to national and international case law, the communications of a person under this protection are covered.

The Belgian Criminal Law states in Articles 259bis and 314bis that the interception of private communications is punishable. These articles also stipulate that the preparation of equipment to intercept such communications as well as the use or trading of information obtained from illegal interception are deemed illegal.

The Electronic Communications Act (ECA) further elaborates on the protection of electronic communications in Articles 122 to 127, and states that it is forbidden to learn about the existence of electronic communications, identity and location of the parties involved and of the content of these communications. It is forbidden to keep track of these communications unless they have been anonymized.

However, the ECA also determines the cases and circumstances in which legal principles of the basic principles can be waived. The ECA determines which electronic communications data should be kept and lists the authorities who can retrieve this information.

The Code of Criminal Procedure and the Security and Intelligence Act provide the powers and circumstances under which competent authorities may request electronic communications information, intercept electronic communications or ask the cooperation of an operator or service provider. These Acts require operators or service providers to cooperate with the prosecuting authorities.

2.3 Code of Criminal Procedure[1]

Art.	Description	Competence
39ter	Conservation of designated data	Criminal investigation officer
39quater §2	Conservation of specified data on demand from a foreign government	police service designated by his Majesty
46bis	Retrieval of data about • Identification of users / devices • Information of services	Crown prosecutor Directly or via a police service designated by his Majesty
88bis	Retrieval of Traffic and location data Both historical and real time	Research Judge State Attorney in certain cases Directly or via a police service designated by his Majesty
90ter 90quater §2	Intercepting communications	Investigating judge State Attorney in certain cases Directly or via a police service designated by his Majesty
90ter 90quater §4	Provide information / cooperation to gain access to communications or systems	Investigating judge State Attorney in certain cases Directly or via a police service designated by his Majesty
464/13	Cf. Art. 46bis but then in the context of a criminal investigation	Judge who keeps track of execution of punishments
464/25	Cf. Art. 88bis but then in the context of a criminal investigation	Judge who keeps track of execution of punishments
464/26	Cf. Art. 90ter but then in the context of a criminal investigation	Judge who keeps track of execution of punishments

[1] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1808111730&table_name=wet
(for investigations and judicial investigations)
http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1808121230&table_name=wet
(for criminal investigations)

2.4 Royal Decree obligation to cooperate in court proceedings

RD 9 JANUARY 2003 - Royal Decree: Terms and provisions for the legal obligation to cooperate in legal warrants relating to electronic communications [2]

Art.	Description
1	Definitions
2	Obligation of CCJ based on Belgian territory Possibility to have a shared CCJ (Collaboration Cell Justice) Security Clearance CCJ members Permanent availability CCJ Notice of information (and amendments thereto) regarding CCJ and members of BIPT Obligation to protect information CCJ and ensure confidentiality
3	Collaboration regarding identifications Article 46bis - appointment NTSU CTIF Powers of NTSU CTIF to access customer data Powers of NTSU CTIF to control this data transfer
4	Collaboration regarding access to traffic and localization data - in real time or historical Timeframe in which to respond to a question Power of government to regulate format and transfer mode
5	Co-operation for interception of electronic communications Indication NTSU CTIF as a central service intercepting communication
6	Obligation to meet government requests Quality requirements of transmitted data: Correlatable, in clear language Real-time forwarding in a secure manner To respect ETSI and 3GPP standards - authority of the government to choose options
8	Obligation to time synchronization of operator systems Accuracy of notified times
10	Provisions concerning investment, exploitation and maintenance costs Reference to attachment for fees
10bis	Authorization of government to determine format and transfer method Obligation to provide information if electronic exchange is not possible
Attachments	Information on cooperation fees Definitions: Query / Query Criterion / Specific Request Fees for performance Annual fee Reaction possibility when requesting accumulation

[2] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2003010942&table_name=loi

2.5 Intelligence Services Act

Act of 30 November 1998 - Act regulating the intelligence and security services [3]

Art.	Description	Competence
18/7	Retrieval of data about • Identification of users / devices • Information of services	Head of service of Intelligence Service Information Officer in certain cases
18/8	Retrieval of Traffic and location data Both historical and real time	Head of service of Intelligence Service Information Officer in certain cases
18/17	Interception of communications	Head of service of Intelligence Service after agreement by BIM (Special Intelligence Methods) committee

2.6 RD Duty to collaborate with warrants provided by the intelligence services

RD 12 OCTOBER 2010 - Royal Decree on the arrangements for the legal obligation (warrant-based) to cooperate with the intelligence and security services relating to electronic communications [4]

Art	Description
1	Definitions
2	Obligation of CCJ based on Belgian territory Possibility to have a shared CCJ Security Clearance CCJ members Permanent availability CCJ Notice of information (and changes thereto) regarding CCJ and members to BIPT Obligation to protect information CCJ and ensure confidentiality
3	Participation for identifications Art. 18/7 Jurisdiction of intelligence services to access to customer data Jurisdiction of intelligence services to regulate this data
4	Participation traffic and localization data - in real time or historical Timeframe in which to respond to a question Power of government to regulate format and transfer mode
5	Cooperation for interception of electronic communications Designation of a network connection point determined by head of service intelligence service
6	Power of government to determine format and way of transfer Obligation to provide information if electronic exchange is not possible
7	Provisions relating to investment, exploitation and maintenance costs Reference to attachment of RD obligation of collaboration legal proceedings for fees for inquiries by intelligence services
8	Obligation to meet government requests Quality requirements of transmitted data: correlated, in clear language Real-time forwarding in a secure manner Respecting ETSI and 3GPP standards - authority of the government to determine options Obligation of time synchronization of operator systems Accuracy of transmitted times

[3] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1998113032&table_name=loi
[4] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2010101212&table_name=loi

2.7 Act on Electronic Communications[5] (ECA)

Act of 13 JUNE 2005. - Electronic Communications Act

Art.	Description
122	Basics of traffic handling (delete / anonymize) And exceptions for: • legal obligation • billing • marketing • fraud detection
123	Basic principles of handling location data and exceptions
124	General Principle of Prohibition of Notice, Identification, Interception, Use of this Information
125	Exceptions to Art. 124 and 259bis and 314bis Criminal Code (Interception) If the Act imposes it • Surveillance on proper operation / execution • Aid and emergency services • BIPT, Investigating judge, Crown Prosecutor, Head of Service VSSE, ADIV • Telecom Ombudsman • Civil Servants of Economics Department • Ethics Committee Telecom • Prevent spam / stalking
126 §1	General obligation of traffic data retention
126 §2	Authorities who may request this information • Judicial authorities • Information and security services • Emergency services • Officers BIPT • Officer Cell Missing Persons (entity of Federal Police) • Telecom Ombudsman
126 §3	Determination of retention period and reference to RD for data
126 §4	Obligations regarding • Quality Warranty and data protection • Security against destruction, alteration, unauthorized access or disclosure • Treatment by members of Coordination cell only • Conservation (retention) within the EU • Technological protection obligation • Keeping a log of usage of stored data
126/1	Obligations to abide by the Coordination Cell • Establishment of coordination cell • Possibility of common coordination cell • Security clearance for members of the coordination cell • Draw up internal procedure for handling questions • Designate a special appointee for protection of personal data
127 §1	Power of government to impose administrative / technical measures regarding user identification
127 §2	Prohibition to replace technology which makes identification / localization /

[5] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2005061332&table_name=loi

	interception impossible
127 §3	Obligations for services with prepaid card

2.8 Royal Decree on retention of data[6]

19 SEPTEMBER 2013. – RD concerning execution of Article 126 of the Act of 13 June 2005 on electronic communications

Art	Description
2	Definitions
3	Concerning fixed telephony: identification information / information on traffic and localisation
4	Concerning mobile telephony: identification information / information on traffic and localisation
5	Concerning Internet access: identification information / information on traffic and localisation
6	Concerning electronic mail services: identification information / information on traffic and localisation
7	Obligations when combining different services required Time stamp precision / synchronisation
8	Obligations concerning the responsible for the protection of Privacy-related information
9	Obligation to provide BIPT with statistics

2.9 RD regarding the identification of users of prepaid cards [7]

RD 27 November2016 regarding identification of end-user of public electronic mobile communications services provided by a prepaid card.

Art.	Description
1	Application field: Telephone number BE / IMSI BE Exclusion of identification: M2M Cards
2	Definitions: document of identification / method of identification
3 – 6	Obligations of end user in identification matter and reporting of theft/loss
7	Basic principles of obligation of identification
8	Obligation of deactivation when notified of theft /loss
9	Obligation of verification using valid identification methods
10	Authorisation through lecture / scan / photograph of identity card
11	Obligatory verification that Belgian identity card BE wasn't stolen or was the object of fraud Actions to take when confronted with irregularities
12	Information that can be retained for the means of identification
13	Obligation to propose at least one valid identification method
14	Terms to physically identify an end user
15	Terms to identify an end user with the electronic identity card
16	Terms to identify a user with the help of an identification service provider

[6] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2013091920&table_name=loi
[7] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2016112703&table_name=loi

17	Terms to identify with the help of an online bank payment
18	Terms when extension of product
19	Terms to identify by means of an electronic communications device

2.10 Ministerial Decree on buffering and filtering of electronic communications – in development

(Project of) Ministerial Decree concerning the execution of Article 6, § 3, sentence two and Article 10bis, sentence two of the RD of 9 January 2003 concerning the terms of compulsory legal collaboration in case of judiciary demands concerning electronic communications

This MD will define the followings terms and conditions:

- The instalment of a buffer capacity by the operators to ensure that in the event of a connection failure between operator and NTSU CTIF, no data will be lost

- Filtering possibilities that an operator has to provide before the data reaches NTSU CTIF. Objective of this filtering is to limit the amount of electronic intercepted data to the strict minimum as requested by the investigating judge.

The MD has already been debated with the concerning players but has yet to be published.

3 Obligations of operators and providers

From the overview of the various legal provisions, we summarize the most important obligations of operators and service providers together.

3.1 In substitution of Coordination (Justice CCJ) [8]

In order to maximize the confidentiality of the investigations of the competent authorities and the privacy of the certified persons, the legislature has chosen to keep the group of people tasked with these assignments as limited as possible with each operator and service provider.

A coordination cell must be established and the contact details must be communicated to BIPT.

Its personnel must be screened in accordance with the procedure described in Art. 126/1 ECA. The safety clearance should be renewed every 5 years.

The Act allows working with different operators and / or service providers with a common CCJ.

The CCJ must be located on Belgian territory. Quid CCJ for service providers located abroad? Obligation to install a CCJ?

Only the members of the CCJ may be aware of the progress of the warrants and may respond.

Only when it is strictly necessary to respond to the question asked in the warrant, members of a CCJ may be assisted by technicians.

3.2 2. Designate an appointee for the protection of personal data [9]

Given the importance that our society dedicates to protecting privacy, every operator and service provider is obliged to appoint a person responsible for the protection of personal data in his firm.

This appointed person must supervise:

- compliance with legal provisions by the company and the CCJ
- that only statutory data are kept
- that only the competent authorities have access to the data stored
- that security and protective measures are in place

The Act allows working with different operators and / or service providers with a joint special appointee for the protection of personal data.

The contact details of this Appointed Person should be communicated to the Commission for the Protection of Privacy.

[8] Art. 126/1, § 1, ECA, Art. 2 RD obligation to cooperate Justice, Art. 2 obligation to cooperate with the intelligence services
[9] Art. 126/1, § 3, ECA

3.3 Providing an internal guideline for cooperation with the authorities [10]

Each operator and service provider must provide an internal directive for its CCJ employees and for assistant technicians explaining within which legal framework this assistance is granted, and which obligations and conditions are to be respected.

3.4 Keeping a log of questions and answers [11]

Each and every operator and service provider must keep a log in which the requests and the answers provided are kept.

This log can be consulted by the Commission for the Protection of Privacy. They can also ask for a copy of it.

3.5 Supply of the annual statistics regarding the requests [12]

3.6 In order to allow the authority to adapt its policy and to distribute the indemnities in a lawful manner, the operators and service providers have to provide BIPT with the numbers regarding their collaboration each year. General data retention

Article 126 ECA determines which electronic communications data should be kept in order to comply with requests for identification of users or communication means and to provide traffic and location data.

The data must be stored within the European Union.

3.7 Data protection

The operator or service provider has to take all the necessary organizational and technical measures to protect data against unauthorized third parties gaining access and to protect these data against destruction, alteration or loss.

3.8 Storage of data at the request of the appointed civil servant [13]

In addition to the general requirement of conservation as explained in the previous paragraph, a police or intelligence officer may also demand that an operator or service provider retains specific data.

The recipient of such a retaining order must preserve the data for a 90-day period that may be extended in writing.

This question will usually be asked to the operator to ensure that a requesting foreign government will be able to receive a satisfactory response as soon as he has sent his international request for legal assistance to the Belgian authorities.

3.9 Destruction or anonymisation of the data [14]

[10] Art 126/1, § 2, ECA
[11] Art 126, § 4, 7° ECA
[12] Art. 9 RD Data retention
[13] Art. 39ter and 39quater, § 4, CIC

As soon as the legal basis for the retention of electronic communications data is lost because the intended period has elapsed, the operator or service provider must delete or anonymize the relevant data as provided for in the basic principle described in Article 122 ECA.

3.10 Obligation to provide information about their services and security [15]

An operator or service provider must provide information to the prosecuting government regarding the services it provides and the ability to access it in clear language.

3.11 Participation obligation to access communications [16]

An operator or service provider must, if requested, provide technical assistance to access electronic communications.

3.12 Provision of identification data and data about services provided

The operator must provide information to a requesting government about:

- the identification of subscribers or users of their services (personal data, address, billing address, contract, etc.)
- the identification of the electronic means of communication used (e.g. IMEI, IMSI, IP, MAC, ...)
- the identification of services to which a person is subscribed or which are being used on a regular basis by a user

3.13 Delivery of traffic and location data

The operator must provide information to a requesting government about:

- the identification of subscribers or users of their services (personal data, address, billing address, contract, etc.)
- the identification of the electronic means of communication used (e.g. IMEI, IMSI, IP, MAC, ...)
- the identification of services to which a person is subscribed or which are being used on a regular basis by a user

3.14 Obligation to intercept and provide intercepted data

An operator or service provider must be able to forward real-time data from a designated electronic communications service to the NTSU-CTIF (Central Technical Interception Facility).

3.15 Time synchronization and accuracy of requested timestamps

[14] Art. 122 and 126, § 4, 6° ECA
[15] Art. 90quater, § 4, and Art. 88quater CIC
[16] Art. 90quater, § 4, and Art. 88quater CIC

Time playing a crucial role in electronic communications, it is imperative that the time setting of all systems involved continuously synchronizes with a reliable time signal such as an atomic clock or GPS time signal.

If timetables are to be related to traffic data, they will be displayed with an accuracy of up to one second.

3.16 Confidentiality obligation

All persons who need to treat the questions in the warrant and the data that form the answer are subject to professional secrecy.

This means that they cannot disclose information about the warrant, the prosecuting government, the question(s) asked, the person(s) concerned, the answer or any other information about this warrant to persons other than those belonging to the CCJ.

If technicians are requested to provide assistance regarding the warrant, then this will be done under the responsibility of the CCJ and only strictly necessary information will be communicated to the relevant technicians.

These technicians are also bound by this confidentiality obligation.

4 Penalties

4.1 Letting disappear, destroy or modify data for which retention is requested

If a person who was asked to retain data destroys, lets disappear or modifies this data, he will be punished with an imprisonment ranging from six months to one year and with a fine of twenty six to twenty thousand euros or with one of those penalties separately.

4.2 Non-compliance with the obligation to retain data as imposed by the Act[17]

In case of non-compliance to retain data as imposed by the Act, the Act stipulates fines up to 50,000 euros.

4.3 Refusal of cooperation or non-cooperation within the requested time

Depending on the requested cooperation, failure to provide the legally required cooperation will be punished by fines or imprisonment.

Likewise, failure to provide the requested cooperation in real time or at the times requested by the competent authority shall be punished equally.

The fines can range from twenty six to twenty thousand euros.

Prison sentences can range from six months to one year.

4.4 Infringement of confidentiality

Any breach of confidentiality by giving for example unauthorized third parties access or giving them some information about the requested cooperation, the persons enrolled, the places or the telecommunications means shall be punished in accordance with Article 458 of the Criminal Code.

Unauthorized third parties in this context are all persons who do not belong to the Coordination Cell.

However, technicians may be enabled to provide special assistance to the members of the Coordination Cell. From that moment on, they are also subject to this confidentiality obligation.

It is therefore important to inform the relevant staff of this confidentiality obligation.

[17] Art. 126 and Art. 145 ECA

5 Compensation fees

5.1 General principles regarding reimbursement of operators and service providers

The attachment to the RD's obligation of cooperation in judicial proceedings determines the compensation provided for the requested cooperation of operators or service providers.

All investments or operating costs incurred by operators or service providers to enable their cooperation with the competent authorities in accordance with the procedures laid down by law or imposed by the government shall be borne by these operators or service providers.

The government compensates only 5 activities with a specific rate: query of historical data, demand for real-time traffic or localization data, survey of cell tower data, request for cooperation for interception of communications and the demand for exceptional requests.

5.2 The specific reimbursed services with compensation

The warrants that give rise to a remuneration per service rendered are:

Point	Service	Compensation
Art. 2, 1°	Observation in real time	€ 92
Art. 2, 2°	Observation of historical data (retro)	€ 80
Art. 2, 3°	Observation in network (Transmission masts / network access points)	€ 115
Art. 2, 4°	Interception of communication	€ 140
Art. 2, 5°	Specific requests See definition in Article 1 of the Annex	Actual costs After submission of evidence

Any operator or service provider delivering one of the services above based on a warrant shall be reimbursed in accordance with this tariff.

5.3 Specific requests

The specific request referred to in Art. 2, 5 °, shall be understood as an exceptional request not mentioned under another item of this Annex and showing such demonstrable form of complexity that the operator of an electronic communications network or the provider of electronic communications services cannot respond to it automatically but only through the intervention of one or more technical experts.

Thus, a specific request does not mean the warrant for the provision of services that fall within the categories of services with a specific tariff or services within the framework of the fee.

For these services, operators and service providers are expected to have optimized their operation so that they can promptly provide the government with the requested service or provide the information so that no further intervention is needed from technicians.

5.4 Other services falling in a flat rate

With the aim of facilitating the processing of warrants and, in particular, facilitating the invoicing of services, all services provided for in the previous rate scheme valid from 2013 to 2016, for which no own specific rate is currently provided, fall within the flat rate.

The services falling under the flat rate are the following:

Copy contract
Copy receipt
Area Coverage map
Identification
Delivery of services purchased by a person
Delivery of services purchased at an address
IMEI track
ISMI track
Identification of a user of an IP address / Notification of a used IP address
Communication of an IP address assigned to a user at a given time/a given period
Operator service track
Point of sale
PUK code
Voice mail reset
Information about recharging
Payment method call originating from a phone cell

5.5 Distinction between large and small operators

The RD's obligation of cooperation in judicial proceedings distinguishes between large and small operators and service providers.

A large operator / service provider is a party that receives more than 4% of the annual number of applications for which no specific rate is provided (and which fall within the flat rate).

All other operators are subject to compensation for unspecified services under the remuneration scheme for small operators.

5.6 The flat-rate services reimbursed by an annual fee for large operators

All other services that fall within the flat rate and cannot be considered as specific requests, and are provided by the major operators on behalf of the judicial authorities, are reimbursed by means of an annual fee.

This lump sum and its distribution are recorded annually by Royal Decree.

For 2017 and 2018 this is set at € 1.3 million.

The distribution of this fee is settled according to a distribution key which will be based on a 5-year moving average of the 5 largest performance amounts. [18]

Currently, only Proximus, Telenet and Orange are considered to be major operators. No other operator or service provider exceeds the 4% stated.

5.7 The fee for small operators

Small operators can receive an annual fee of € 1,000 for the service to the judicial authorities if they:

- Have communicated their data from their Coordination Cell to BIPT
- Engage and prepare for using the TANK exchange platform

6 Role NTSU-CTIF

Art. 46bis and 88bis Sv state that the authorities cannot only direct their questions to operators and service providers, but can also do so through a police service appointed by his Majesty.

Art. 1, 3 and 10bis of the RD's obligation of compulsory legal proceedings indicate the NTSU-CTIF as this service.

Art. 3, 4, 5 and 6 of the RD's obligation of information disclosure determines that the intelligence service provider may determine the way in which the information is to be provided.

Since 2003, the NTSU-CTIF has been the administrator of the central interception infrastructure within the framework of judicial investigations. Since 2010, the CTIF infrastructure is also used for interceptions carried out on demand from intelligence services.

The NTSU-CTIF will run the TANK project

	Availability	Contact Details
Permanently available Staff CTIF	24/7 via telephone	02 642 77 11 DSU.NTSU.CTIF.PERM@police.belgium.eu
Permanently available staff ICT CTIF	24/7 only through perm CTIF	DSU.NTSU.CTIF.IT@police.belgium.eu

7 Regulatory authority for the exchange of information

By virtue of Art. 10bis of the RD cooperation requirements judiciary requests and Art. 6 of the RD cooperation requirements intelligence services the government has the opportunity to determine the mode and format of the data exchange.

By virtue of Art. 10bis of the RD cooperation requirements judiciary requests and Art. 6 of the RD cooperation requirements intelligence services the government may choose options among the ETSI and 3GPP standards to standardize the format and the data transfer.

8 Project Tank

8.1 General description of the project

[18] As these services no longer have tariffs of their own, the distribution key is calculated based on the tariff in force from 2013 to 2016.

The TANK2.0 project will provide for the development of the automated exchange of questions and answers between the police and intelligence services on the one hand and the operators and service providers on the other hand.

The users of the police or intelligence services will have access to this application by means of an internal website in their normal working environment and in accordance with a claim from a competent authority, will be able to upload the demands and add the corresponding warrants. Via the same way, they will be able to download the data as soon as they are available.

As soon as the question is submitted, it is handled by TANK, with a unique number and formatted in a specific digital format.

The operators will either be able to pick up this request from the TANK Web server or receive these requests via Web services. Once they have been processed, operators will be able to post their response to the same Web server or transfer through Web services.

The operators and service providers working with the TANK Web server will be notified by mail whenever a new question is available.

TANK will strive to automate a maximum number of question types, including real-time observation questions and interception requests. The operator concerned will then transfer this information in response to these requests to the Central Interception Infrastructure of the government.

The registration of the queries and replies in TANK will provide the basis for supporting the payment of services with a specific rate on the one hand and for the calculation of the distribution key of the annual fee for large operators on the other.

8.2 Architecture

Finally, the architecture of the exchange platform will be determined in the development phase. Basically, the architecture of TANK is:

- A database that stores questions, justification documents, answers received.
  The answers will only be saved for a limited time until verification by the applicant.
- A Web server with Web application for the requesting users
- A Web server with Web application for the operators
- A mail server that will send messages each time new questions are available
- A Web service platform for a fully automated encrypted exchange of questions and answers between TANK and fully integrated operators

8.3 Determination of standard response formats

To put an end to the different response formats currently used by operators and service providers, the project will primarily seek to determine a fixed answer format for the different types of questions. This format must be respected regardless of the operator or service provider.

8.4 Planning the project

The preliminary study of the project TANK took place in 2016. In May 2017 the development of the project will start with an expected development time of approximately one calendar year.

The development will be done in two stages:

Phase 1: development of database Web applications for users and operators, mail services and the automation of the questions regarding identification.

Scheduled completion phase 1: Q4 2017.

Phase 2: development of Web services for automated data exchange with major operators, the further automation of other questions including questions for real-time monitoring and interception.

Scheduled completion phase 2: Q2 2018

8.5 Integration possibilities with TANK

It is clear that the need for integration into the TANK system will depend on the number of questions that operators receive annually. To prevent a costly integration for small operators and to enable new operators immediately into the operational processes of the government, two options have been taken into consideration:

- "Light integration": the operator or service provider only uses the Web application and will be notified by mail of the fact that a new request has arrived.
- "Full integration": for each type of question it will be possible to arrive at an automated exchange of questions and answers based upon Web services.

In the first place the "full integration" is only provided for the major operators or service providers. If a small operator or service provider, however, estimates that the number of questions he must process is sufficiently high to switch to "full integration" for certain types of questions, then he will address this demand to NTSU CTIF. After an evaluation of this demand, it will be decided whether the request will be granted.

Depending on the progress of the development, questions will first be made available only through the Web application. Subsequently
.....

Operators or service providers will therefore be asked to work via the Web application for certain types of questions and through Web services for other questions.

8.6 Cooperation requirements regarding TANK

Although the current legal framework provides direct questioning and a search through an intermediate party, it is the intention of the government to process all queries with TANK. Once TANK as an exchange platform has been put in place, the relevant legal provisions will be further adjusted to this effect.

All operators, whether they are small or large operators, will therefore eventually be obliged to cooperate with the government through the exchange platform TANK.

To cooperate with TANK it is necessary that such operator or service provider:

- provides the contact details of its Coordination Cell Justice and its members

- employs as members of the CCJ people with a security clearance
- provides an e-mail address with the following structure TANK.CCJ@providername.extension
- guarantees that the mailbox will be checked regularly to gain knowledge of new demands
- collects via the Web application every new notification mail corresponding to a new demand
- compiles the answers according to the format determined by government
- compiles the answer files according to a format that will be announced later

The engagement will go further, for those operators who want “a full integration”

- The development of integrated applications that will communicate through Web services with TANK
- The integration with the central system for interception for demands of observation in real time and the interception of telecommunications

9 Engagement with a view to obtaining an annual flat fee as a small operator

9.1 Identification of the operator

Name Company	
Type of operator	
Type of services provided	
Address	
Contact	
Contact phone	
Contact e-mail	
VAT No.	
Mandate signed	

9.2 Notification of CCJ and contact details

I confirm that the aforementioned company:

- has taken note of the obligations and requirements imposed by law on operators and service providers;
- has installed a CCJ and that contact information was sent to BIPT;
- has filed an application for a safety clearance for members of the CCJ;
- has taken the necessary steps to meet the legal requirements.

9.3 Appointment of Appointee for protection of personal data

I confirm that the above company:

- Engaged appointees for the protection of personal data
- Has submitted the contact details for these appointees to the Commission for the Protection of Privacy

9.4 Commitment to cooperate through the TANK platform

I confirm that the above company:

- has taken note of the information about the project and about the TANK principles for data exchange of questions and answers regarding the warrants provided by the authorities
- is committed to let its CCJ cooperate with the exchange platform TANK as soon as it is available and that the answers will be delivered in the format determined by the government.

9.5 Application for reimbursement as a small operator

The undersigned requests in accordance with Article 3 of the Annex to the Royal Decree Cooperation obligation the application for reimbursement as a small operator

Done at …….. on ……/……/2017 Signature