Information brochure for operators

Police

Information brochure for operators

This brochure aims to inform the heads of service and the staff of the operators' coordination cells about the practicalities of responding to the requests from law enforcement agencies.

Recipients	Heads of Coordination Cell & their staff; Police officers
Published by	National Technical & Tactical Support Unit (NTSU) – Federal Police
Case managers	Robin Meutermans & Elodie Bormans
Contact details	DSU.NTSU.DR@police.belgium.eu
Issue date	28/04/2026
Reference N°	NTSU-2026/753
Classification	Public

Executive summary

This brochure was conceived by the NTSU (National Technical and Tactical Support Unit) of the federal police. The goal of this document is to answer the many questions on the legal and practical aspects that arise from new operators as well as the existing ones. Note that it is an update and an extension of the 2017 version[1].

After having set the overall context of the duty to collaborate to judicial investigations on the side of the operator, we explain here in detail several topics: primarily the practical background, the legal background, the technical background, as well as financial aspects.

A better understanding of these topics should help novice operators build their cooperation with authorities, mainly with the NTSU.

Please note that this brochure has been written from the perspective of judicial authorities and does not take into account the modalities of other authorities.

Practical background

When we talk about the practical side, we refer to the different parties involved in the cooperation and their respective obligations. We discuss further in this section the role of the NTSU, of the operators and mainly their coordination cells, and of the authorities.

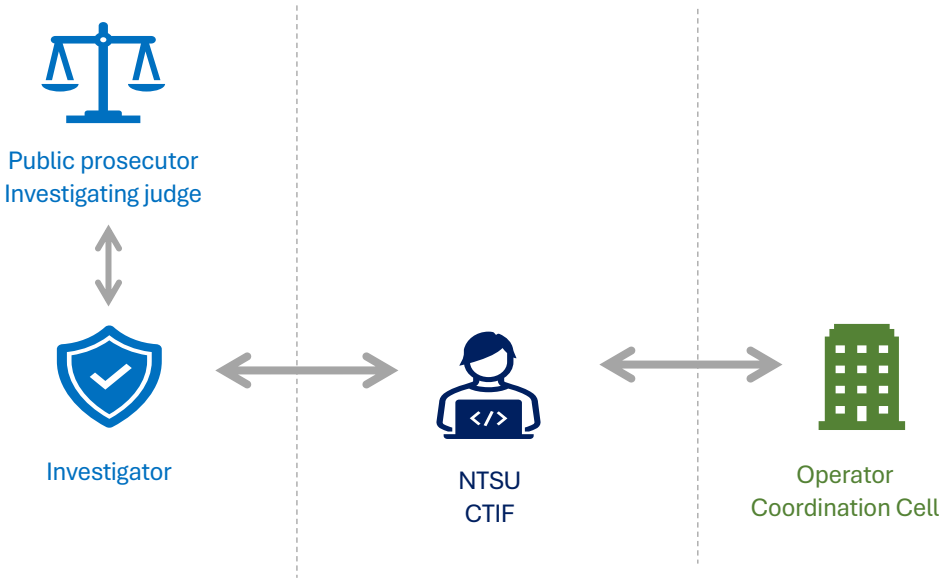


Figure 1: *Relevant stakeholders of judicial cooperation*

Within the NTSU, operators mainly interact with the CTIF (Central Technical Interception Facility). This is the single point of contact within the federal police for treating all requests regarding identification, localisation and interceptions of electronic communications. This section explains in more detail the modalities related to these types of requests, also referred to as 'measures'.

[1] NTSU (2017). *Legal obligations to cooperate for network operators and providers of electronic communications services*. BIPT. (Link)

CTIF is in direct contact with the respective Coordination Cells (CC) at the operator side. This cell is responsible for collecting the responses and transmitting them to the requesting authority. According to Belgian legislation, every operator is required to have a coordination cell.

The requesting authority is the authority that orders a measure and receives the results. However, not every authority is authorised to request data from operators, so we provide a list of those authorities that are authorised to do so.

Legal background

Naturally, we wouldn't expect the operators to act without the necessary legal safeguards and provisions. However, the list of applicable legislation can become quite extensive. Therefore, we provide an exhaustive list of all the applicable laws and decrees. The most notable are the code of criminal procedure (art. 46bis, 88bis, 90ter) and the law on electronic communications (articles 122 to 127/3).

Technical background

Besides the legal background, it is also important to understand what exactly will be expected from the operators. In this section we elaborate what technical details are required for each type of measure. We provide an exhaustive list of what information an operator should receive from the requesting authority and what result the operator is expected to provide the authority.

In a nutshell, by identification we mean the identification of a subscriber or the identification of the services to which a person is subscribed. Localisation, and additionally observation, we refer to the tracing of traffic data of a device or the localisation of the origin or destination of electronic communications. Finally interception regards the recording and intercepting all communications (voice, SMS, MMS, data) in real time.

Financial background

Finally, we address the financial aspects for the operator when cooperating with the competent authorities. These are governed by the royal decree of November 8, 2016, which sets out the reimbursement procedures for service fees, complex requests, and an annual flat rate.

Table of contents

1 General introduction on the duty to cooperate

Today, where almost everyone uses electronic means of communication and information systems, it is a necessity for the various authorities to be able to conduct investigations in this "virtual" environment as well. Only when law enforcement is provided with the right tools of investigation, can the rights of society and citizens be respected, and can suspects be traced, identified, located and, if necessary, can information be obtained about their communications.

These investigations would not be possible without the cooperation of network or electronic communication service operators (hereinafter referred to as "operator").

To this end, the legislator has granted various competences to certain authorities and intelligence services on the one hand and imposed various obligations on operators on the other.

When implementing the legal provisions, authorities such as the police, the public prosecutor's office, and regulatory bodies work together with operators to establish effective cooperation and ensure compliance with the law. The authorities aim to make this cooperation as efficient and economic as possible. For these reasons, the National Technical & Tactical Support Unit (hereafter NTSU) of the Federal Police was designated as the competent intermediary for the exchange of requests and answers between the authorities and the operators for a number of types of cooperation.

An exchange platform called TANK (“Telecom Automation National Knowledge centre”) has been developed to automate information exchange. Connecting to this exchange platform as an operator is not only important for a swift information exchange but is also a crucial condition for the operator to be reimbursed for its cooperation.

This document provides a brief overview of the legal framework, competences, obligations of operators, sanctions, the role of different authorities, the exchange platform and the request for operators’ commitment.

This document does not at all pretend to be exhaustive. It is a starting point for anyone who needs to acquire knowledge about the cooperation between government departments and operators. We hope that this brochure may improve the cooperation between concerned parties.

It is not required to read the entire document when needing information on a particular topic. Whether the reader is part of the coordination cell (CC), the legal department or the technical department within the operator, this brochure was written with three sections in mind: the coordination cell (part 2), the legal department (part 3), the technical department (part 4) and the financial aspects (part 5). It is possible to skip between sections without missing essential information.

2 Practical modalities for the coordination cell

This section describes the different actors involved in the collaboration between authorities and operators. On one side there is NTSU and the competent authorities. NTSU, as part of the federal police and the intermediary between operators and authorities, is responsible for the execution of the requests and the authorities are competent for originating the requests. On the other side there is the operator, specifically their coordination cell, who are responsible for providing the necessary data as answer to the requests.

2.1 Role of NTSU

Art. 46bis and 88bis of the Code of Criminal Procedure (CCP) state that the law enforcement authorities can not only address their requests directly to the operators, but can also do so through a police service designated by the King. Article 1 of the royal decree on data conservation (see point 3.1.7) designates the NTSU as this service. This royal decree authorises the NTSU to act as an intermediary between operators and judicial authorities.

Since 2003, the NTSU, more specifically the CTIF (Central Technical Interception Facility) has been the administrator of the exchange platform and the central interception infrastructure in the context of judicial investigations. Since 2010, the CTIF infrastructure has also been used for interceptions carried out on the request of the intelligence and security services.

The main missions of the NTSU consist of the covert collection of information, through technical means and infrastructures, and the distribution of the collected data to police investigators and external partners such as intelligence and security services (ADIV and VSSE). CTIF's cooperation can be requisitioned in judicial investigations, tactical operations and crisis situations. CTIF's role takes place in the domain of 'taking cognisance of private communications'.

2.2 Role of CTIF

2.2.1 General introduction

This subdivision of the NTSU is responsible for processing requests and carrying out the technical aspects of an identification, localisation and interception of electronic communications in Belgium.

By ensuring the centralised administration of the data concerned, CTIF provides essential support in a national and sometimes international context to the federal and local police and other authorities. CTIF is therefore a key link in the work of the law enforcement, security and intelligence services, and their missions have a general impact in the fight against the most serious criminal threats.

CTIF carries out its responsibilities through close collaboration with operators by ensuring that an efficient, secure and reliable infrastructure is in place at all times, and by providing training and assistance to the end users.

The interception of electronic communications requires different systems using the most advanced technologies. Consequently, CTIF has its own infrastructure for this purpose, which they manage and develop. Over the years, CTIF has acquired the development capacity to implement their own solutions in order to make intercepting electronic communications more effective.

2.2.2 Functioning

CTIF is the central point for the execution of interception, observation and localisation measures regarding telecommunications and is therefore contactable 24/7. The role of CTIF is be divided into 3 missions.

Contact details	(+32) 02 642 77 11 DSU.NTSU.CTIF.PERM@police.belgium.eu

The **first** mission of CTIF centres around the daily management of the exchange platform TANK, where they function as the General Functional Administrator (GFA), i.e. a helpdesk for both investigators and members of the coordination cells (CC) within the operators. Their responsibilities include assisting investigators and CC members in navigating the application, documenting issues related to requests, exploring potential solutions for notified problems (primarily concerning access rights), and directing inquiries to the relevant services. They also manage CC user rights such as creating new members, resetting passwords, and resetting QR codes. Furthermore, their role entails reviewing performance statements generated by operators and conducting tests to ensure the application operates as expected. Upon request, the CTIF may also review audit logs.

Additionally, the role of CTIF involves monitoring the access to the application for several purposes. Firstly, verifying the rights of public authorities' usage, which consists of checking if the user has the necessary rights in TANK, whether the user is registered on a list of authorised users in their unit, and if the user list is linked to the case the user wants to access. Also, it includes examining what government users are able to view in their case to identify and explain any issues they encounter, both as the user requesting assistance and as the administrator of their unit. Their responsibilities also extend to creating, managing, activating, or deactivating CC users, reviewing monthly performance reports generated by various TSPs, creating test files, inputting test requests.

Similarly to exchange platform TANK, CTIF serves as a central service for the interception facility. They execute the same role for the interception facility, as they do for the exchange platform (e.g. access rights, problem resolution), with the addition that CTIF also supervises the execution of the interception measures themselves. This means that, instead of the investigator registering the measure, as they would have done in the exchange platform, it is the members of CTIF who create and follow-up the measure in the interception facility system.

The **second** mission can be defined as their 'IT role'. CTIF acts as both front and back-end for the exchange platform and for the interception facility systems. Their role as 'IT support' is extremely varied, though their core business is the maintenance of the general infrastructure. Their tasks range from monitoring the systems and servers and making sure that everything is up and running, to the development of the exchange platform TANK and the interception facility, which require updates and software development. They are also responsible for the integration of the operators' systems in the exchange platform TANK and the interception facility.

International requests are CTIF's **third** mission. Aside from their role in the exchange platform, the interception facility and as IT service, CTIF also is the Single Point of Contact (SPOC) for international judicial requests to online service providers (OSP), such as Google, Apple, Facebook, Amazon, Microsoft, etc. They play a pivotal role in the transmission of requests and answers between investigators and OSP. Due to the complicated nature of the collaboration with international OSP, there currently doesn't exist an integrated exchange platform like TANK. CTIF is required to input the inquiries in the individual portals of the OSP.

2.3 Role of the operators and the coordination cell

2.3.1 Legal definition

Access to the electronic communications market is entirely free. However, the legislator has decided that, in order to exercise an activity in Belgium, an operator must be registered with the Belgian Institute for Postal Services and Telecommunications (BIPT). This obligation only applies to operators offering a number-dependant interpersonal communication service.

Under Belgian law, an operator is defined as being a *"person or enterprise providing a public electronic communications network or an electronic communications service available to the public"* (Art. 2, 11° Telecom law).

Articles 46bis and 88bis of the CCP also provides that *"anyone who makes available or offers, by any means, a service within the Belgian territory, which consists in transmitting signals via electronic communications networks, or which consists in allowing users to obtain or receive or disseminate information via an electronic communications network. This includes the provider of an electronic communications service."*

In addition, we also refer to the definition under the recent e-Evidence Regulation[2], where the legislator states that any company offering electronic communications network/services is bound to adhere to the law in question.

Finally, we refer to the definition provided by the European Electronic Communications Code: *'operator' means an undertaking providing or authorised to provide a public electronic communications network or an associated facility* (article 2 (29)).

2.3.2 MNO, MVNO and OTT

To avoid any misunderstanding, it is important to clarify that there are three types of operators and that they cannot produce exactly the same data.

1. MNO = Mobile Network Operator (e.g. Orange, Telenet and Proximus)
   MNO's are independent operators who own a complete telecom infrastructure (including a radio spectrum license, a wireless network infrastructure, etc.) for hosting and managing electronic communications.
   - Possible requests: Identification, services, localisation/observation, and interception. Details about these requests can be found in section 4 of this document.

2. MVNO = Mobile Virtual Network Operator (e.g. Lyca Mobile, BICS, VOO, Mobile Vikings, Scarlet, City mesh)
   The term 'virtual' indicates that these operators do not have their own radio infrastructure and enter into an agreement with a MNO in order to obtain access to their network. They will therefore not be able to provide all the same data as a MNO.
   - Possible requests: Identification, services. Any request requiring network information, such as activation period of a number on a network or activated masts, cannot be answered by a MVNO.
   - A MVNO can, for example, not provide an IMEI- or MSISDN-track, because only operators of a network can obtain this information.

[2] Given the wide scope and complex nature of the e-Evidence Regulation and the accompanying Directive, this brochure will be limited to what is mentioned in point 3.1.16.

3. **OTT** = Over The Top operator (e.g. Telegram, Microsoft, Meta), also known as Online Service Providers (OSP)
   This category of operators do not operate a network, nor do they have licence agreements with any MNO. They offer their services using publicly available internet networks.
   - Possible requests: identification, traffic data and preservation of data.
   - Because of the international nature of the services of OTT, there is no possibility to send a request to an OTT using the TANK platform. The service CTIF International Request, within NTSU, is responsible for handling these requests. Therefore they will not be further discussed in this document.

2.3.3 Coordination Cell (CC)

All operators, active on Belgian territory, are obligated to cooperate in order to execute the requests based on a formal inquiry from a competent authority as already mentioned. In order to facilitate this cooperation, article 127/3 §1 of the LEC (Law on electronic communications, point 3.1.3) stipulates that every operator must establish a coordination cell.

The establishment of a CC contributes to the maximization of the confidentiality of the competent authorities' investigations and the privacy of the targeted individuals. Therefore, the legislator has chosen to keep the group of people carrying out the assignments within each operator as limited as possible. Only the members of the CC may take notice and respond to the inquiries. If strictly necessary for the performance of the advanced service, the members of the CC may be assisted by specialised technicians.

Each CC is required to communicate their contact details to the BIPT. Its staff must be screened in accordance with the procedure described in art. 127/3 §2 LEC and obtaining a security clearance. This is an absolute requirement for all CC members. The royal decree on cooperation obligations in judicial proceedings (see point 3.1.4) explains further that this cell must be located within the Belgian territory and be available 24/7.

Furthermore, the possibility exists for operators to establish a common coordination cell or to delegate this task to another operator. In this regard, the idea is that multiple operators can be represented by the same CC or that a bigger operator assumes this function for a smaller operator. Scarlet, for example, who has no CC, has their requests treated by Proximus. Important to note also is that this delegation can be a complete or partial delegation (see the example given above concerning the MVNO and the MSISDN-track).

2.3.4 Other obligations

We briefly outline several additional obligations for the operators.

2.3.4.1 Internal directive for cooperation

Each operator has to establish an internal procedure for processing the authorities' requests for access to end-users' personal data. They have to provide the BIPT, upon request, with information on these procedures, the number of requests received, the legal basis invoked and the response.

2.3.4.2 Journal

Each operator must keep a journal recording the requests and the responses. This journal should record the identity of the person who consulted the data, the time of the consultation and what data was consulted.

This journal can be consulted by BIPT as well as the Inspector General and their appointed inspectors within the Data Protection Authority. They can also request a copy of it.

2.3.4.3 Providing annual statistics

In order to enable the Government and Parliament to adapt its policy and to be able to distribute remuneration in a justified manner, operators must, at BIPT's request, provide statistics on the supply of data transmitted to the authorities.

The statistics are sent to the Minister for Justice and the Minister for Telecommunications, for subsequent transmission to the Parliament.

2.3.4.4 Preservation of data

Article 126 of the law on electronic communications specifies which data on electronic communications must be kept in order to respond to requests for identification of users or means of communication.

Subscriber identity data and electronic communications metadata must be stored within the European Union (art. 127/2 § 3, 1° LEC).

2.4 Competent authorities

2.4.1 Authorities using the exchange platform TANK and the interception facility

There are several competent authorities who can request data from the operators. The following table presents the subset of them who are fully integrated in the exchange platform TANK.

Table 1: *Competent authorities using the exchange platform and interception facility*

Authorities that may require the cooperation of operators	Services that execute the requests
Authorised magistrates: - Members of the Public Prosecutor's Office - Investigating judges	Federal police Local police
Chief Executive Officer (VSSE) and his delegated officers	VSSE (State Security)
The Head of the SGRS and his delegated officers	SGRS (Intelligence and Security Service)

2.4.2 Exhaustive list of competent authorities

As explained operators are expected to provide all requested information, to the extent that they process it, to the requesting authority. However, not every authority is authorised to request all types of data. The possibility of requesting data must be defined in the organisational law of each authority. Therefore, table 2 shows a brief overview of the competent authorities and the data they are allowed to request.

It should be noted that it is up to the requesting authority itself to verify the correctness of its inquiry. For more information regarding the competent authorities, we refer to the circular letter from the minister of telecom (see point 3.1.14).

Table 2: *Full list of authorities competent to request data from operators*

Authority	Data art. 122, 123 LEC	Data art. 126, 127 LEC	Data art. 126/1, 126/3 LEC
Judicial authorities	Yes	Yes	Only for serious crime (art. 127 §1 1°)
Federal police's missing persons unit	Yes	Yes	Yes
Intelligence and security services	Yes	Yes	Yes
The Belgian Competition Authority (BCA)	Yes	Yes	No
The Financial Services and Markets Authority (FSMA)	Yes	Yes	Only for serious crime (art. 127 §1 1°)
The Inspection Service of the Directorate General Animals, Plants and Food of the Federal Public Service Health, Food Chain Safety and Environment	Exclusively identification data	Exclusively identification data	No
Office of the ombudsman for telecommunications	Exclusively identification data	Exclusively identification data	No
Inspection services of the FPS Economy (E2, E6, E7)	Yes Subject to certain exceptions	Yes Subject to certain exceptions	Only for serious crime (art. 127 §1 1°)
Judicial police officers of the BIPT	Yes	Yes	Exclusively for the control of the telecom law
BIPT as administrative authority	Yes	Yes	Exclusively for the control of the telecom law
The Centre for Cyber security Belgium (CCB)	Yes	Yes	Yes
The General Direction of Statistics - Statistics Belgium of the FPS Economy	Data relating to access, use and financial accessibility of telecommunications services		No
Emergency services providing on-site assistance	Yes	Yes	Yes

2.4.3 Minimum requirements in data requests from authorities

The requests that the authorities send to operators in order to obtain certain data must include the following minimum information[3] :

1) The identity of the requesting authority or, where the request is sent to the operator by a central service on behalf of that authority, the identity of that service;
2) The position of the contact person at the requesting authority or, where the request is sent to the operator by a central service on behalf of the authority, the position of the contact person at this central service;
3) The legal basis for the request, except where the request is sent to the operator via a central service on behalf of another authority;
4) The desired response time.

When registering a request, the investigator must follow several obligations[4]. These requirements should allow the operator to ascertain whether the request is legitimate.

- The investigator must attach to each request the warrant which constitutes the legal basis for the request.
- If the investigator is working on the basis of an oral order from a competent authority, they enter this information in the system and then submit the written request as soon as it is available, thus confirming the oral order even if the request has received a response in the meantime.
- Scans of the competent authority's warrant must be downloaded in PDF format.
- The request must at least mention the following:
    - Exact name of the operator(s) from whom the data are requested
    - The category of data that are requested
    - The intended purposes
    - The (internal) control mechanisms

The written request must always be signed. An operator must refuse any request that is not signed. If the signature is electronic, it must meet the relevant legal requirements. Please note that a signature below an email does not meet these requirements. These requirements can be found in the circular letter from the minister of telecom (see point 3.1.14).

2.5 The exchange platform TANK and the interception facility

Now that the actors are known, we go into further detail about the platforms that are used to facilitate this collaboration between operators and authorities.

On the one hand, there is the exchange platform TANK, which is used for transiting requests between authorities and operators. On the other hand, there is the interception facility, which executes the interception of private communications.

[3] Article 127/1, § 6, Law of 13 June 2005 on electronic communications

[4] Article 127/1, § 5, Law of 13 June 2005 on electronic communications

2.5.1 TANK

Users in the police or intelligence services can enter the inquiries and add the corresponding requests via an internal website available in their normal working environment. On the same site, they will be able to download the data as soon as it is available.

After the request is registered, it is then processed by TANK, given a unique number and formatted in a specific digital format. Operators can then either consult this request on the TANK web server or have it forwarded via a machine-to-machine mechanism known as web services. After processing, operators can post their response on the same web server or transfer it via web services. Operators working through the TANK web server are notified by e-mail whenever a new request is available.

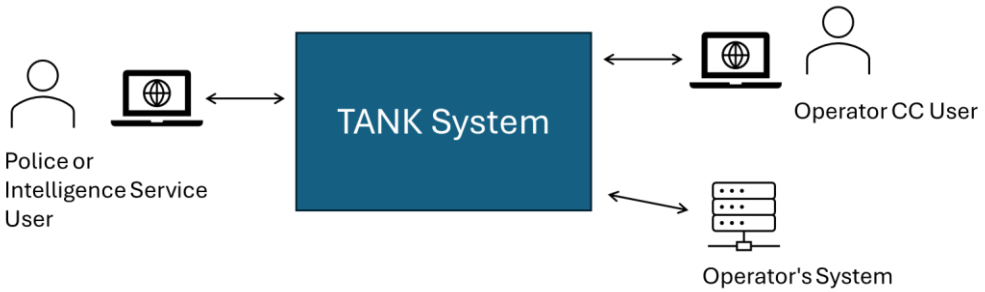


Figure 2: *Diagram of the workflow between the investigator and the operator*

TANK aims to automate as many types of requests as possible. The information contained in the response to these requests should be sent by the operator to the governments' central interception infrastructure. The registration of the requests and responses in TANK is the basis for supporting the payment of specific rates on the one hand and for calculating the distribution key of the annual flat rate on the other.

In summary, TANK aims to:

- Have an automated exchange of requests and answers between the authority and Belgian telecommunications operators
- Enhanced authentication of all parties in the process
- Increase speed and reduce processing errors
- Standardise the format of requests and answers (international standard: ETSI)
- Enhanced data security
- Reduce and recover legal costs (overview of costs per case) (see section 5)
- Simplify invoicing and control
- Have the possibility of auditing the entire process

2.5.1.1 Functioning

The exchange platform consists of two integration levels: the light integration and the full integration.

The light level of integration to the exchange platform works as follows:

- the exchange platform notifies the operator by email of a new request from an authority;
- the request is made available on the exchange platform;
- the operator responds to the request via the same exchange platform;
- Operators respond to the inquiry in either XML format or XLS (Excel file standardised by CTIF).

The full level of integration to the exchange platform works as follows:

- the exchange platform sends the authority's new request via web services to the operator, who acknowledges receipt;
- the operator sends the response to the request via web services to the exchange platform, which acknowledges receipt;
- Operators respond to inquiries in XML format.

TANK supports the standard Excel response format, which is identical to the converted responses of the major operators. The obligation for operators to respond in the standard format (or ETSI XML) has come into effect when the new royal decree on data conservation (see point 3.1.7) was published.

The standard format is intended to standardise operators responses. It allows TANK to automatically identify results and redirect requests to the operators indicated in the standard format response, as it does for the ETSI XML responses of the major operators. It will no longer be necessary to create new inquiries with manual operator selection.

When selecting an operator in TANK, the choice is most often automatic, based on the range of numbers that was attributed to the operator by the BIPT. In that case the NTSU-CTIF has configured the request transfers so that the right operator automatically receives the request. Exceptionally, it could be possible that an operator has to be selected manually.

2.5.1.2 The order of priority

To facilitate the processing of requests, the authorities are asked to assign priority levels to their inquiries. This allows the operators to quickly identify the most urgent requests. The operator processes the request submitted via the exchange platform according to the order of priority given to it.

Table 3: *List of priorities for hte processing of requests*

Routine	Processed during office hours In the order in which the requests were sent (“first in / first out”) No later than the end of the second working day following receipt of the request
Urgent	Processed during office hours Priority treatment before routine requests In the order in which the requests were sent No later than the end of the first working day following receipt of the request
Very urgent	Processed immediately Priority over all other requests Treatment outside of office hours

Requests to which no priority has been assigned are considered to be "routine" applications and ‘office hours’ should be understood as 8 a.m. to 5 p.m. on weekdays, excluding public holidays.

2.5.1.3 Practical modalities

Although the current legal framework provides for a direct request and a request through an intermediary, it is the government's intention to eventually have all inquiries go through TANK. At present, the development of the exchange platform does not yet allow all types of requests to go through TANK, but this remains the intention for the future.

In order to cooperate via TANK, it is necessary that the operator must at least:

- Communicate the contact details of its Coordination Cell and its members
- Request security clearance for all members of the CC
- Provided a mail address with the following structure TANK.CCJ@providername.extension
- On a permanent basis, check this mailbox to be informed of new queries
- As soon as a notification e-mail for a new request arrives, collect it via the web application
- Compile the answers according to the format determined by the government
- The answer files will be formed according to the agreed standard format
- Place the answers on the TANK web server via the web application

For operators looking to build full integration, the commitment goes even further with:

- The development of integrated applications that communicate with TANK's web services
- The connection with the central interception infrastructure (see point 2.5.2)

2.5.1.4 Summary

Table 4: *Summary of the processing of a request via or outside of the exchange platform*

Requesters	Intermediaries	Receivers
Via TANK		
Police investigators → With prior permission from public prosecutor or investigating judge Intelligence and security services → With prior permission from Chief Executive Officer (VSSE) or Head of the SGRS	CTIF CTIF IT	Operators → via their Coordination Cell
- Identification of MSISDN - Track MSISDN > IMEI - Track IMEI > IMSI / MSISDN - Identification ICC ID - Identification IMSI - Track IMSI > IMEI	- History MSISDN - History IMEI - History IMSI - … Roll out in 2026-2027 (see annex 1 for full schedule)	
Outside TANK		
Police investigators → With prior permission from public prosecutor or investigating judge Intelligence and security services → With prior permission from Chief Executive Officer (VSSE) or Head of the SGRS Administrative authorities → After prior verification	CTIF Intelligence and security services Administrative authorities	Operators → via their Coordination Cell
- All other requests		

2.5.2 The interception facility

By providing centralised management of intercepted data, CTIF offers specialised support, in a national or even international context, to the Belgian integrated police and intelligence services.

It does this via a connection to the State Security surveillance room (VSSE), the army's surveillance room (SGRS) and the multiple surveillance rooms of the integrated police.

The interception service offered by CTIF is based on a centralised facility. The interception facility is a software infrastructure used to intercept private communications. It consists of specialised software developed by a private firm. The interception facility application is installed on PCs located in the interception rooms of the PJF and certain local police zones. The interception measure is processed in the listening rooms using the tool provided by CTIF. The start of an interception is be based on a request from an investigating judge

The central interception facility is managed by CTIF for:

- The reception of data from operators following a request from the authorities regarding the obtaining of real-time location or real-time interception of the content of electronic communications;
- The temporary storage of this data;
- The transmission of this data to the requesting authority.

The CC transmits the aforementioned data to the central interception facility in real time, unless otherwise specified in the request.

2.5.2.1 Functioning

It goes without saying that communications intercepted and sent to the central interception facility can only be intercepted if a request has been sent to the operator in accordance with the respective laws.

The judicial warrant will be sent by the investigator, via the CTIF, to the operator. This document contains of the necessary information, in particular:

- Start and end date of the measure
- Number/device to be intercepted
- Responsible police officer
- Case name

The start of an interception measure via the interception facility must be based on a request.

Table 5: *Overview of the legal basis for an observation and interception*

	Art. 88bis CCP	Art. 90ter CCP
What ?	▪ Incoming or outgoing electronic communication traffic. ▪ Location of the origin or destination of the electronic communication.	▪ Intercept, take cognizance of, explore and record means of telecommunication.
How ?	▪ In normal circumstances: written request. ▪ Emergency: verbal order. CTIF requests written proof declaring the existence of this order.	▪ In normal circumstances: written request. ▪ Emergency: verbal order. CTIF requests written request declaring the existence of this order.
Who ?	▪ Investigating Judge ▪ Public Prosecutor in case of flagrante delicto to be confirmed by the	▪ Investigating Judge ▪ Public Prosecutor only if: - terrorist attack

	Investigating Judge within 24 hours except if - terrorist attack - hostage taking/kidnapping - extortion	- hostage-taking/kidnapping - extortion - and lasts only as long as the crisis

A measure will automatically be terminated when the one-month period expires, unless an extension is issued before this date. On the other hand, if a measure needs to be terminated before the one-month period expires, the investigator needs to inform the CTIF in writing.

2.5.2.2 Practical modalities

For the application of an interception measure, the operator has to take the necessary actions, through its Coordination Cell, to ensure that the private electronic communications referred to in the written or verbal request from the competent authority are intercepted and recorded, as soon as the request is received, unless otherwise stipulated in the request.

The judicial authorities and the intelligence and security services are the only ones who can benefit from the central interception facility, as only they can be provided with the content of electronic communications.

The actual execution of an interception or observation in real time always requires the collaboration of the electronic communications operator. The central interception facility only receives data transmitted by the operator.

Only operators who exceed a certain threshold of interception requests or who have obtained NTSU approval (despite being below the threshold) connect to the central interception facility. This means that an operator will be permanently connected to the central interception facility if it carries out more than 24 interceptions per calendar year at the request of the judicial authorities or the intelligence and security services.

Any operator who is not permanently connected to the central interception facility still has to be able, at the request of the competent authorities, to execute an interception request and transmit the intercepted data to the NTSU.

Similar to the exchange platform, the interception facility also has the options of light or full integration. Full integration in this regard means both mobile and fixed devices and both data and voice. Light integration means that an operator is connected to the interception facility for a specific type of interception measure (e.g. fixed voice or fixed data). The operator then makes the intercepted data available on an FTP server managed by CTIF and in principle updates the data 1x per day.

3 Legal background for collaboration

The legal framework within which an operator is bound to cooperate with the government is described in the Telecom Law[5] (which was amended by the Data Retention Law of 2022[6]) and several executive royal decrees (RD) and Ministerial Decrees (MD).

This chapter gives an overview of the most important articles in these laws and RD/MDs with a brief description of their content. A more in-depth reading of these articles is necessary for operators so that they can appreciate their full scope [7].

Moreover, this overview is limited to the cooperation with judicial authorities and intelligence and security services. Certain other authorities also have options for requesting information from the operators, but this document does not elaborate on this.

3.1 Listing of relevant legislation

3.1.1 Code of Criminal Procedure (CCP)[8]

The Code of Criminal Procedure (CCP) is the base legal document in regards of criminal proceedings. It outlines the procedures and rules to be followed in the investigation and prosecution of criminal offenses. It includes provisions for arrest, search and seizure, interrogation of suspects, trial procedures, sentencing, etc.

As this document pertains to the procedures concerning electronic communications, we focus on the provisions relating to investigations and judicial enquiries, namely the articles 46bis, 88bis and 90ter. The articles 464/13, 464/25 and 464/26 should also be considered as they relate to sentencing procedures.

3.1.2 Law on Intelligence Services[9]

Police investigations will be referencing the above mentioned articles of the CCP. The intelligence service however will have their own organic law, with the most important articles being 18/7, 18/8 and 18/17.

3.1.3 Law on Electronic Communications (LEC)

The 2005 Law on Electronic Communications (LEC, a.k.a. Telecom law) has already been revised several times over the years. The most recent and (for the purposes of this brochure) most important amendment took place on 08/08/2022 when the Data Retention Law was published.

Most notably are the articles 122 to 127/3, as these articles describe the current data retention regime.

[5] 13 JUNE 2005. – Law regarding electronic communications law

[6] 20 JULY 2023. – Law on the collection and conservation of identification data and metadata in the electronic communications sector and their transmission to authorities

[7] We also refer here to the questions and answers exchanged during several consultation moments between the operators (led by ISPA and BCPA) and the authorities.

[8] Code of Criminal Procedure – First book & Second book

[9] 30 NOVEMBER 1998. – Law regulating the intelligence and security services

3.1.4 Royal decree on cooperation obligations in judicial proceedings[10]

This royal decree (RD) describes the modalities for the legal obligation to cooperate in judicial proceedings relating to electronic communications.

In the future this RD will almost entirely be repealed and replaced by the RD 'TANK' (point 3.1.8).

3.1.5 Royal decree on cooperation obligations in proceedings of the intelligence and security services[11]

This RD explains the modalities for the legal obligation to cooperate in proceedings of the intelligence services relating to electronic communications.

In the future this RD will be almost entirely repealed and replaced by the RD 'TANK' (point 3.1.8).

3.1.6 Royal decree on prepaid cards[12]

This RD details the identification of the end-user of a mobile public electronic communication service provided on the basis of a prepaid card.

3.1.7 Royal decree on data conservation[13]

This RD replaces entirely the RD from 19/09/2013 and informs the operators on certain details for the retention by electronic communications operators of data for authorities under articles 126 to 126/3 of the LEC and statistics on the communication of these data to authorities.

Additionally, it is important to note that this RD designates NTSU as competent intermediary authority.

3.1.8 Royal decree on the exchange platform TANK and interception facility[14]

As the title partly explains, this RD stipulates the use, functioning and access regarding the exchange platform TANK and interception facility.

This RD has not yet been published and is currently being discussed on the level of ministers.

[10] 9 JANUARY 2003. – Royal decree on modalities for the legal obligation to cooperate in judicial proceedings relating to electronic communications

[11] 12 OCTOBER 2010. – Royal decree on modalities for the legal obligation to cooperate in proceedings of the intelligence services relating to electronic communications

[12] 3 May 2024. Royal decree amending the royal decree of 27 November 2016 on end-user identification of mobile public electronic communications services provided on the basis of a prepaid card

[13] 4 OCTOBER 2023. – Royal decree on the retention of data by electronic communications operators for the authorities in accordance with Articles 126 to 126/3 of the Law of 13 June 2005 on electronic communications and statistics on the communication of such data to the authorities

[14] Royal decree regulating the transmission by electronic communication operators of electronic evidence to the Belgian competent authorities and for its freezing

3.1.9 Royal decree modalities for the legal obligation to cooperate[15]

The annex of this RD stipulates the reimbursement rates for the operators who process requests from judicial authorities. It describes both the reimbursement for services provided and a flat rate.

3.1.10 Royal decree on ministerial authorisation in the context of 5G network deployment[16]

This RD establishes the obligation for any operator to seek ministerial authorisation when employing a 5G element. Included in this RD is the obligation to request authorisation from the competent minister when an operator plans to collaborate with a *high risk vendor.*

3.1.11 Ministerial decree (MD) on geographical zones[17]

This MD establishes the list of judicial arrondissements and police zones subject to the data retention obligation, together with the retention period.

Since the law of 20 JULY 2022 requires annual validation of the statistics, used for the determination of the above mentioned list, as per art. 126/3 of the LEC by the COC (Supervisory Body for Police Information). This MD is amended annually.

3.1.12 Ministerial decree on critical infrastructures

As provided for in art. 45 of the Data Retention Law, an MD will be published by 01/01/2027 at the latest, which, in addition to the aforementioned geographical zones, will also determine the zones of critical infrastructures (as referred to in art. 126/3 §§3-6 Telecom Law).

This MD is currently still in the preparatory phase, so we cannot elaborate further on it here.

3.1.13 Ministerial decree on buffering and filtering of electronic communications[18]

This MD defines the ETSI standards that need to be used in order to avoid data loss and the transmission of non-relevant data.

3.1.14 Circular letter from the minister of telecom[19]

The circular falls within the scope of art. 127/1 §5 2nd paragraph of the LEC and includes a list of Belgian authorities authorised to receive data from an operator, as well as general considerations intended to help operators and competent Belgian authorities in the context of data retention requests.

[15] 8 NOVEMBER 2016. - Royal decree amending the royal decree of 9 January 2003 on modalities for the legal obligation to cooperate in judicial requests relating to electronic communications, on the rates for the remuneration of cooperation

[16] 16 APRIL 2023. - Royal decree on ministerial authorisation in the context of 5G network deployment

[17] 28 MARCH 2024. – Ministerial decree implementing article 126/3, § 1, of the Law of 13 June 2005 on electronic communications with a view to establishing the list of judicial arrondissements and police zones subject to the data retention obligation, together with the retention period

[18] 9 JULY 2020. – Ministerial decree implementing article 6, § 3, second paragraph, and article 10bis, second paragraph, of the royal Decree of 9 January 2003 containing the on modalities for the legal obligation to cooperate in judicial proceedings relating to electronic communications

[19] 1 MARCH 2024. – Circular letter from the Minister for Telecommunications of [date] on the transmission by operators to the competent Belgian authorities of identification and metadata retained pursuant to articles 122, 123, 126, 126/1, 126/3 and 127 of the Electronic Communications Law

3.1.15 Digital Services Act (DSA)[20]

The Digital Services Act aims to create a safer online environment for consumers and companies in the European Union. The regulation introduces responsibilities and a system of accountability and transparency for providers of intermediary services. The DSA also introduces the concept of Very Large Online Platforms (VLOP) and Very Large Online Search Engines (VLOSE).

We focus your attention mainly on Article 10, which introduces the "orders to provide information".

3.1.16 E-Evidence Regulation[21] and Directive[22]

E-Evidence establishes two main concepts. Firstly, the Regulation establishes the legal grounds for authorities to request data from international service providers. Secondly, the Directive sets out the obligation for service providers, who offer services in the EU, to designate a legal representative in one of the member states.

The transposition of both the regulation and the directive is currently being discussed on the level of ministers

3.1.17 NIS2 Directive[23]

This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market. To that end, this directive establishes measures and obligations on cybersecurity risk-management, information sharing and cybersecurity strategies.

This European directive has since been transposed into Belgian law through the law on cyber security of network and information systems[24].

[20] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC

[21] 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

[22] Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings

[23] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148

[24] 26 APRIL 2024. - Law establishing a framework for the cybersecurity of network and information systems of general interest for the public security

4 Technical background

4.1 Introduction

Before going into detail about what type of requests an operator can expect from authorities, we provide here an overview of all the data parameters that are inscribed in the telecom law (see annex 2 for a complete overview). Of course, not all data can be requested at all times, it depends on the request type.

Table 6: *Overview of identification data*

Identification data			
Customer identification	**Technical details**	**Identification of services**	**Payment details**
Name	CGI	Provider ID + name	Billing address
Date + place of birth	MSISDN	Redirected provider	Type of payment
Nationality	IMEI	ID + name	Method of payment
National registry number	IMSI	Subscription	Date of payment
Authentication (identification) document	SUPI	Subscription type	Reference of payment transaction (in case online)
Issuing Country	SUCI	Start and end of subscription	Surname/first name (in case online)
Name of company	PEI	Line status	Address (in case online)
Address	MAC address	Call attempts without result	Date of birth (in case online)
	IP address	Call forwarding or transfer	
	Same details for addressee	Redirected number	

Table 7: *Overview of observation and localisation data*

Observation & localisation data			
Traffic data			**Network Connection**
Outgoing communication (voice/SMS & PSTN)	**Incoming communication**	**Data (incl. 5G)**	
MSISDN target	MSISDN (at the origin of the incoming call)	Date, time	Switch on equipment
MSISDN addressee		IMEI	Switch off equipment
Date, hour		SUCI/SUPI/…	Activity on network
Location pylon		IMSI	
Start-/end time		Protocol	
Name provider		Volume of data	
IMSI		MAC address	
"IMEI + type/brand of device"		Data types	
(e)(raw) CGI		IP address (when making a data call)	
Technology used			
Type technology			
Antenna			

We also include the interception data. Contrary to identification, localisation and observation data; the telecom law does not address the interception of content data. However, the CCP does allow law enforcement and intelligence and security services to request an operator to intercept the communications of one of its subscribers.

Table 8: *Overview of interception data*

Interception data	
Content data	User account data
Content of communication (Voice, SMS, MMS, data)	All data linked to user account
Traffic data	
Holder of number/device	
Mast localisation	

In general, three types of requests can be distinguished, each linked to a specific article in the Code of Criminal Procedure:

1. Art. 46bis: Identification
2. Art. 88bis: Observation and localisation
3. Art. 90ter: Interception

For each type of request, we specify in the following section what an operator can expect from an investigator and what the investigator expects from the operator. It is important to understand that in practice the investigator will enter the request in TANK based on a written warrant from either a public prosecutor or an investigating judge. So while it is the public prosecutor or the investigating judge that requests data parameters, it will be the investigator who executes the request in TANK.

4.2 46bis – Identification

A request for an identification emanates normally from a public prosecutor and relates to identifying a number (MSISDN, IMSI, etc.), a subscriber, a service or others.

Generally, a public prosecutor can request the following:

1. The identification of a subscriber;
2. The identification of the services to which a person is subscribed.

In case of an extreme urgency, this request can also be given orally by the investigative judge, but it must always be followed up as soon as possible with a written request.

Table 9: *Details of identification data*

Type of request	What will the investigator provide to the operator?	What is the expected result from the operator?
Phone number IDN-01	Mobile-, fixed-, fax number	The identification of the holder. As well as all the elements* that allow to proceed to the identification of the holder.
IP address IDN-02	IP address, start-/end date	Identification of the holder of the subscription linked to the IP address active for a specific period.
ICCID IDN-03	ICCID number	The identification of the associated MSISDN and/or IMSI of the SIM card. As well as all elements that allow to proceed to the identification of the holder.
MAC address IDN-04	MAC address	Identification of the holder of subscription and localisation of connection linked to device with this MAC address.

SSID IDN-05	SSID	Identification of the holder of subscription and localisation of connection linked to access point with this SSID.
IMSI IDN-06	IMSI number	The identification of the holder. As well as all the elements that allow to proceed to the identification of the holder.
MSISDN > IMEI TRACK TRK-01	MSISDN number, start-/end date	Activation periods on the telephone network for the number for a specific period.
IMEI > IMSI/MSISDN TRACK TRK-02	IMEI number, start-/end date	IMSI or MSISDN numbers which have been linked in the GSM box bearing the IMEI number, with identification of holders of those cards for a specific period.
IMSI > IMEI TRACK TRK-03	IMSI number, start-/ end date	Different GSM boxes (IMEI) which have been used with SIM card bearing the IMSI number for a specific period.
Phone number SRV-01	Mobile-, fixed-, fax number	The identity of the holder of the number Subscriptions, products and/or services linked to telephone number. As well as all the elements that allow to proceed to the identification of the holder.
Person SRV-02	Surname, first name, date of birth, National Registration Number, Authentication number	The associated number(s), subscription(s) and/or services. As well as all the elements that allow to proceed to the identification of the holder.
Company SRV-03	Company name, VAT number, Company number	The associated number(s), product(s), subscription(s) and/or services. As well as all the elements that allow to proceed to the identification of the holder. If requested: statements of invoices, Copy of contracts / ID DOC, recharge method.
Address SRV-04	Building number, street name, postal code	The number(s) associated with the address. As well as all the elements that allow to proceed to the identification of the holder.
Extra MSISDN – PUK CODE EXT-01	MSISDN number	PUK code (PUK1/PUK2 – 4 to 8 digits) to unlock the SIM card linked to the MSISDN number. As well as all the elements that allow to proceed to the identification of the holder.
Extra MSISDN – Copy of contract EXT-02	MSISDN number, start-/end date	Copy of the contract linked to the MSISDN number for a specific period. As well as all the elements that allow to proceed to the identification of the holder.
Extra MSISDN – Payment information EXT-03	MSISDN number, start-/end date	Payment information linked to the MSISDN number for a specific period. As well as all the elements that allow to proceed to the identification of the holder.
Extra Cover map EXT-04	CGI number, a set of CELL ID numbers	Map of cell coverage (mast, relay antenna)

* When referring to “all the elements”, this also includes:

Table 10: *Details of subscriber and device data*

Type information	Elements	Examples
Subscriber information	Name	Peeters, Jan
	Address	Luchtmachtlaan 10, 1040 Etterbeek
	Date of birth	20020510
	Date of creation of the customer	20100625
	Type of authentication	Passport, eID, drivers licence
Subscription information	Service provider reference	3601 *(number assigned by BIPT)*
	Subscription reference	Type of subscription e.g. Fibre 100 or Dolphin Max 15GB
	Subscription date	20230101
	Contract end date	20231231
	Phone number assigned to the person associated with the contract	00324981547854
	ICCID number (if sim-card is present)	893200 22 2222 222222 8
	IMSI number (if available)	313 460 000 000 001
	Associated e-SIM cards	ICCID number of E-SIM
	Type of subscription	Prepaid, Postpaid or other
	Type of connection	Fibre, DSL or other
	The means of payment (account number linked to the direct debit)	Debit, transfer, prepaid IBAN number, BIC number, SEPA reference
	The installation address (equipment)	Ruiterijlaan 2, 1040 Etterbeek
	IP address: period for which the IP address has been assigned, option/restriction linked to the contract	From 20240201 12h34 until 20240201 15h20 Fixed IP address, max 3TB/month
Device information	MAC address	00:1B:44:11:3A:B7
	DSL identifier	406472
	IMEI number	350123451234560
	Router, modem, PC network card (+ associated IP address)	IPv4: 192.158.1.38 IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
	List of connected objects (using a router)	Nest Cam D8:EB:45:4B:F9:80 ip: 192.168.0.101

4.3 88bis – Observation and localisation

A request for an observation or localisation emanates from an investigating judge and relates to the location of persons or devices, as well as incoming/outgoing calls, the activation of masts and others. In short, localising and observing the whereabouts of a person or device.

Generally, they can request the following:

1. Tracing the traffic data of an electronic communication device from or to which electronic communications were made;
2. Locating the origin or destination of electronic communications.

The investigating judge must issue a duly motivated request stating the factual circumstances of the case justifying the measure, taking into account the proportionality and subsidiarity of the requested measure. This request must also mention the duration of the measure, which cannot exceed two months starting from the request.

In particular cases the investigating judge can request data for a period of 12 months (in cases of terrorism), 9 months (in cases of organised crime) or 6 months (for other criminal offences) preceding the request.

In case a crime is discovered while it is being committed, the public prosecutor can likewise order a measure, only for the offences mentioned in art. 90ter. In this case, the measure must be confirmed by the investigating judge within 24 hours. Such a confirmation is not necessary if the crime consists of terrorism, hostage-taking, deprivation of liberty or extortion.

In case of an act of terrorism, a public prosecutor can request the measure within 72 hours of the discovery of this offence, without the confirmation of an investigating judge.

In case of an extreme urgency, a request can be given orally by the investigating judge, but it must always be followed up as soon as possible with a written request.

Within the legal framework of article 88bis, we can identify three main requests:

1. **HIS** [History] = requests to obtain data for a period in the past that ends on or before the day the measure is requested.
2. **DEX** [Daily execution] = Requests to obtain the previous day's historical data for a period starting no earlier than the day the measure is requested.
3. **OBN** [Observation] = Requests for real-time traffic data for a period in future, starting at the earliest when the day the measure is requested.

Table 11: *Details of observation and localisation data*

Type of request	What will the investigator provide to the operator?	What is the expected result from the operator?
Phone number HIS-01	Mobile-, fixed-, fax number; start-/end date Including foreign numbers	Details of* data connections, incoming and outgoing calls related to the number, with identification of holders and localisation of masts activated for a specific period
IMEI HIS-02	IMEI number, start-/end date	Details of data connections, incoming and outgoing calls related to the number, with identification of holders and localisation of masts activated for a specific period
IMSI HIS-03	IMSI number, start-/end date	Details of data connections, incoming and outgoing calls related to the number, with identification of holders and localisation of masts activated for a specific period
Location HIS-04	Adress/set of coordinates, start-/end date	Details of data connections, incoming and outgoing calls which have transited through any mast covering the zone(s), with identification of holders and localisation of masts activated for a specific period
CELL ID HIS-05	CELL ID number, start-/end date	Details of data connections, incoming and outgoing calls which have transited through mast with the Cell ID number, with identification of holder for a specific period
IP address HIS-06	IP Address, start-/end date	Details of IP traffic linked to the address for a specific period
Phone number - Copy of invoices HIS-07	Mobile-, fixed-, fax number; start-/end date	Copy of the invoices related to this number
Route HIS-14	A set of waypoints, start-/end date	Details of data connections, incoming and outgoing calls that transited through any mast

		covering the waypoints in the order in which they were provided and for a specific period
Phone number in real time DEX-01	Mobile-, fixed-, fax number; start date Automatic daily requests will be sent	Details of data connections, incoming and outgoing calls related to the number, with identification of holders and localisation of masts activated for a specific period
IMEI DEX-02	IMEI number, start date Automatic daily requests will be sent	Details of data connections, incoming and outgoing calls related to the number, with identification of holders and localisation of masts activated for a specific period
IMSI DEX-03	IMSI number, start date Automatic daily requests will be sent	Details of data connections, incoming and outgoing calls related to the number, with identification of holders and localisation of masts activated for a specific period
IP address DEX-04	IP address, start date Automatic daily requests will be sent	Details of IP traffic linked to the address for a specific period
Phone number OBN-01	Mobile-, fixed-, fax number; start-/end date	*Real-time* details of incoming and outgoing calls related to the number, with identification of holders for a specific period
IMEI OBN-02	IMEI number	*Real-time* details of incoming and outgoing calls related to the IMEI number, with identification of holders and localisation of activated masts for a specific period
Identifier (dsl ID) OBN-03	DSL identifier	*Real-time* details of data items linked to the identifier for a specific period

* When referring to "details of", the data listed below are what is expected.

- Subscriber details (name, address, date of birth, subscription information – See 4.2)
- The identification/creation data of the user
- The IP address at the time of creation with the date, time, and time zone
- The history of activations/connections of an account/number for the requested period
- Date, time, duration of the call/communication

4.3.1 Signalling data

A particular aspect of observation or localisation is a request for signalling data. This is a relatively new type of request, introduced by article 126/2 §2 of the Telecom law. Similar to a localisation request the legal basis is article 88 CCP and the request emanates from an investigating judge (or a public prosecutor, in exceptional cases).

Signalling data might be requested when the results of a classic request for localisation data doesn't provide sufficient clarity.

Type of request	What will the investigator provide to the operator?	What is the expected result from the operator?
Signalling data	MSISDN number; start-/end date	All locations and/or alerts for the MSISDN number which are processed in an electronic communications network

The authorities will be informed that a gradual approach is most favourable. Meaning that in a first instance a basic localisation or observation request should be introduced and after review of the results they can proceed to request signalling data, for a specific period of time and for no more than 24 hours.

4.4 90ter – Interception

A request for an interception emanates from an investigating judge and always relates to obtaining the content of a communication; such as text messages, a phone call or others.

This measure can only be ordered in exceptional cases: if there are serious indications that it concerns an offence referred to in paragraph 2 of article 90ter, and if other means of investigation are not sufficient to establish the truth.

Article 90quater states that any measure taken based on article 90ter is subject to prior written authorisation, with reasons, from the investigating judge, which is forwarded to the public prosecutor. This authorisation indicates notably the period during which the measure may be executed, which may not exceed one month.

The investigating judge may extend the measure one or more times (article 90quater, § 1) for a further period not exceeding one month, with a maximum of six months.

In the event of discovery during a criminal act, and as long as the offence lasts, the public prosecutor may order an interception measure for offences regarding terrorism, hostage-taking or extortion by force or threat. For offences of terrorism (excluding the threat to commit such offence), the public prosecutor may order an interception measure within seventy-two hours of the discovery of such offence. Authorisation may be given verbally and must be confirmed in writing as soon as possible.

Table 12: *Details of interception data*

Type of request	What will the investigator provide to the operator?	What is the expected result from the operator?
Phone number TAP-01	MSISDN number (fixed and mobile), IMSI number; start-/end date Including foreign numbers	Recording and intercepting all communications (voice, SMS, MMS, data) during their transmission linked to the number, interception of traffic data, with identification of the holders and localisation of masts activated for a specific period
IMEI TAP-02	MSISDN-/IMSI number; start-/end date	
User account TAP-03	Identifiers of a user account, start-/end date	Interception of data linked to a user account for a specific period

4.5 Example of how a judicial investigation proceeds

Example 1

A person is suspected of being part of a criminal organisation and having committed an armed robbery. The operator is asked to carry out an interception on his mobile phone (art. 90ter).

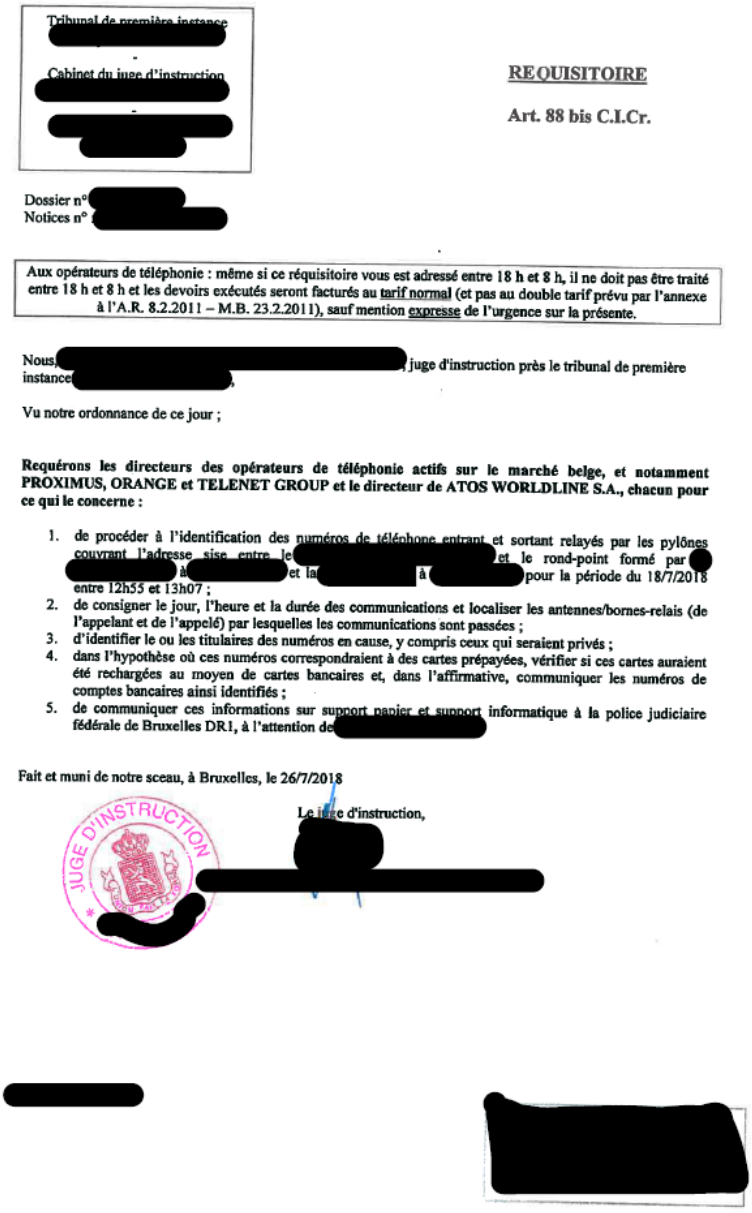
From the analysis of the interception results, it becomes clear that the man has a second mobile phone. A request* (art. 88bis) is then sent to the network operators asking them to (1) identify the incoming and outgoing telephone numbers that passed through masts covering a specific address, (2) register the day, hour and duration of the calls and locate the antennas through which the calls were made, (3) identify the holder(s) of the numbers in question.

Based on the results received from the operators, the investigators are able to determine two numbers that corresponded to the mast and duration of the communication.

Finally, a history is requested for the two new numbers as well as a localisation of the antennas used (art. 88bis) and an interception measure for one of the numbers (art. 90ter).

Ultimately, based on the results and analysis of this information, the perpetrator could be traced and arrested.

* This is the request used for the article 88bis in this investigation :



Tribunal de première instance
[redacted]
Cabinet du juge d'instruction
[redacted]

REQUISITOIRE

Art. 88 bis C.I.Cr.

Dossier n° [redacted]
Notices n° [redacted]

Aux opérateurs de téléphonie : même si ce réquisitoire vous est adressé entre 18 h et 8 h, il ne doit pas être traité entre 18 h et 8 h et les devoirs exécutés seront facturés au tarif normal (et pas au double tarif prévu par l'annexe à l'A.R. 8.2.2011 – M.B. 23.2.2011), sauf mention expresse de l'urgence sur la présente.

Nous [redacted], juge d'instruction près le tribunal de première instance [redacted],

Vu notre ordonnance de ce jour ;

Requérons les directeurs des opérateurs de téléphonie actifs sur le marché belge, et notamment PROXIMUS, ORANGE et TELENET GROUP et le directeur de ATOS WORLDLINE S.A., chacun pour ce qui le concerne :

1. de procéder à l'identification des numéros de téléphone entrant et sortant relayés par les pylônes couvrant l'adresse sise entre le [redacted] et le rond-point formé par [redacted] à [redacted] et la [redacted] à [redacted] pour la période du 18/7/2018 entre 12h55 et 13h07 ;
2. de consigner le jour, l'heure et la durée des communications et localiser les antennes/bornes-relais (de l'appelant et de l'appelé) par lesquelles les communications sont passées ;
3. d'identifier le ou les titulaires des numéros en cause, y compris ceux qui seraient privés ;
4. dans l'hypothèse où ces numéros correspondraient à des cartes prépayées, vérifier si ces cartes auraient été rechargées au moyen de cartes bancaires et, dans l'affirmative, communiquer les numéros de comptes bancaires ainsi identifiés ;
5. de communiquer ces informations sur support papier et support informatique à la police judiciaire fédérale de Bruxelles DR1, à l'attention de [redacted]

Fait et muni de notre sceau, à Bruxelles, le 26/7/2018

Le juge d'instruction,

JUGE D'INSTRUCTION

[redacted]

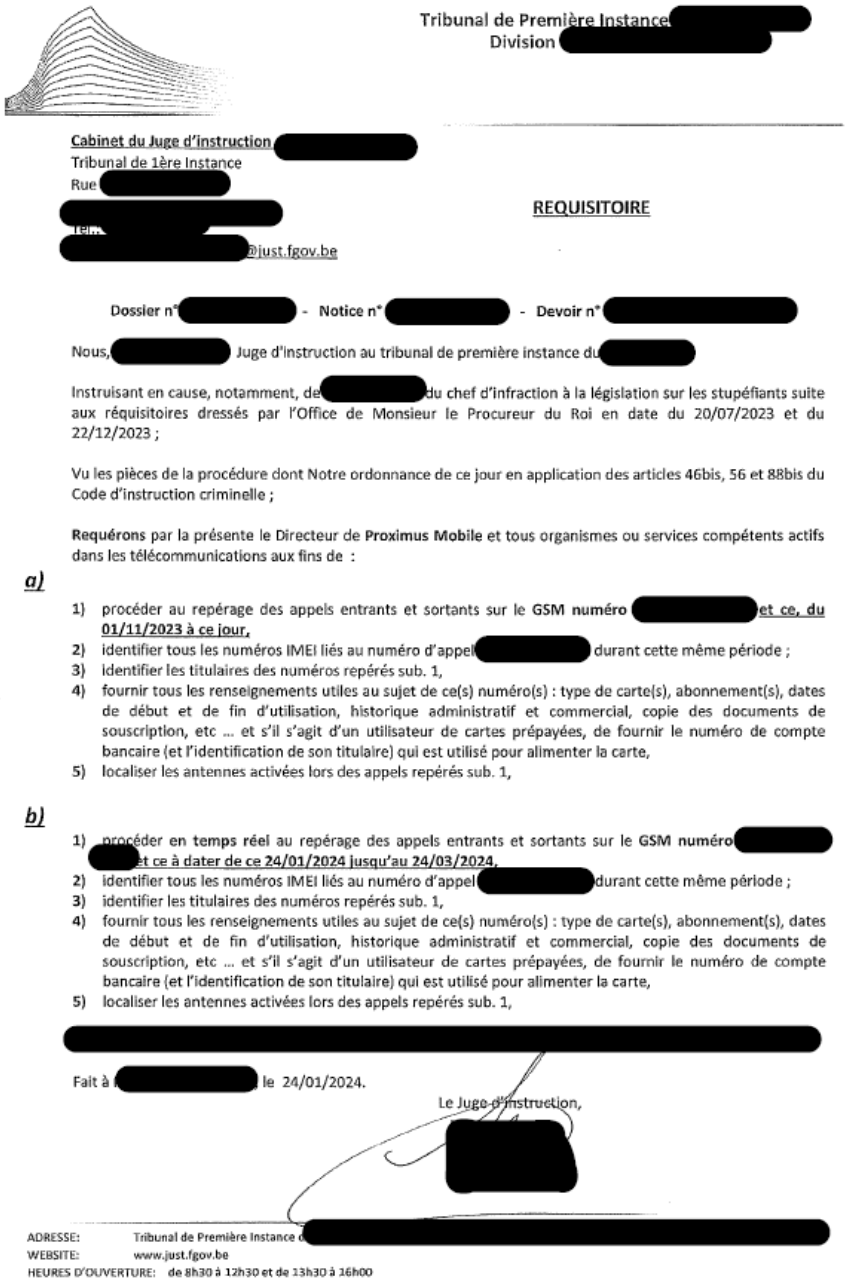
Figure 3: Example of a judicial warrant relating to art. 88bis CCP

Example 2

An drugs-related crime has been committed but the identity of the perpetrator is unknown. The only thing investigators can base their research on is a mobile phone number that was used during the crime.

The investigators solicit* the operator to (1) trace incoming and outgoing calls on the mobile phone for a specific period of time (art. 88bis), (2) identify all the IMEI numbers linked to the number during this same period (art. 46bis), (3) identify the holders of the identified numbers (art. 46bis), (4) locate the antennae activated during the identified calls (art. 88bis) and (5) provide all relevant information about the number(s) (art. 46bis).

* This is the request used in this investigation :



Tribunal de Première Instance [redacted]
Division [redacted]

Cabinet du Juge d'instruction [redacted]
Tribunal de 1ère Instance
Rue [redacted]
[redacted]
Tél. [redacted]
[redacted]@just.fgov.be

REQUISITOIRE

Dossier n° [redacted] - **Notice n°** [redacted] - **Devoir n°** [redacted]

Nous, [redacted] Juge d'instruction au tribunal de première instance du [redacted]

Instruisant en cause, notamment, de [redacted] du chef d'infraction à la législation sur les stupéfiants suite aux réquisitoires dressés par l'Office de Monsieur le Procureur du Roi en date du 20/07/2023 et du 22/12/2023 ;

Vu les pièces de la procédure dont Notre ordonnance de ce jour en application des articles 46bis, 56 et 88bis du Code d'instruction criminelle ;

Requérons par la présente le Directeur de **Proximus Mobile** et tous organismes ou services compétents actifs dans les télécommunications aux fins de :

a)

1) procéder au repérage des appels entrants et sortants sur le **GSM numéro** [redacted] **et ce, du 01/11/2023 à ce jour,**
2) identifier tous les numéros IMEI liés au numéro d'appel [redacted] durant cette même période ;
3) identifier les titulaires des numéros repérés sub. 1,
4) fournir tous les renseignements utiles au sujet de ce(s) numéro(s) : type de carte(s), abonnement(s), dates de début et de fin d'utilisation, historique administratif et commercial, copie des documents de souscription, etc … et s'il s'agit d'un utilisateur de cartes prépayées, de fournir le numéro de compte bancaire (et l'identification de son titulaire) qui est utilisé pour alimenter la carte,
5) localiser les antennes activées lors des appels repérés sub. 1,

b)

1) procéder **en temps réel** au repérage des appels entrants et sortants sur le **GSM numéro** [redacted] **et ce à dater de ce 24/01/2024 jusqu'au 24/03/2024,**
2) identifier tous les numéros IMEI liés au numéro d'appel [redacted] durant cette même période ;
3) identifier les titulaires des numéros repérés sub. 1,
4) fournir tous les renseignements utiles au sujet de ce(s) numéro(s) : type de carte(s), abonnement(s), dates de début et de fin d'utilisation, historique administratif et commercial, copie des documents de souscription, etc … et s'il s'agit d'un utilisateur de cartes prépayées, de fournir le numéro de compte bancaire (et l'identification de son titulaire) qui est utilisé pour alimenter la carte,
5) localiser les antennes activées lors des appels repérés sub. 1,

[redacted]

Fait à [redacted] le 24/01/2024.

Le Juge d'instruction,

[redacted]

ADRESSE: Tribunal de Première Instance [redacted]
WEBSITE: www.just.fgov.be
HEURES D'OUVERTURE: de 8h30 à 12h30 et de 13h30 à 16h00

Figure 4: *Example of a judicial warrant relating to art. 46bis and 88bis CCP*

4.6 Particularities

4.6.1 Missing warrants

Oral requests should be followed by a written warrant as soon as possible, even if the request has already been executed.

There are a few mechanisms in place to uphold this obligation:

- Weekly reminders to all investigators who have yet to supply a warrant
- When a warrant is not available, an explanation needs to be provided

Please note that it is the responsibility of the requesting party to provide all necessary documents.

4.6.2 Missing responses

It is the responsibility of the operator to respond to the requests of authorities.

In the next version of TANK 2 new options will be added:

- "Missing warrants": the operator has the possibility to select this status and thus inform the authority that a warrant still needs be provided
- "Remark": if a warrant is provided, an operator cannot refuse to respond. However, the addition of a 'remark' or 'comment' allows the operator to communicate any doubts they might have regarding a warrant.

If an operator regularly refuses to collaborate, the authority can inform BIPT about this situation. Being the regulatory body for the electronic communications market, BIPT can, in the worst case scenario, impose sanctions on an operator who neglects their obligation to collaborate.

5 Financial aspect

TANK not only offers a national platform for efficient exchange of requests and answers, but also a means for operators to seek compensation for their collaboration with the authorities. However, an invoice can only emanate from the operator who was identified in the TANK-system as the provider in the scope of the request.

The royal decree of 08/11/2016 (see point 3.1.9) lays down the fees provided for the requested cooperation of operators. Beware, all investments or operational costs that operators must incur to enable their cooperation with the competent authorities within the modalities provided for by law or imposed by the government are borne by these operators.

5.1 Reimbursements for services

In accordance with the RD, the requests that give rise to a fee per service provided are:

Table 13: *Overview of the costs for the execution of judicial requests*

Type of request	Fee
Transmission of metadata received in real time for one request criterion[25]	€ 92
Transfer of metadata history for one request criterion	€ 80
Transferring the history of metadata for a given location at one or several access point(s) of an electronic communications network	€ 115
Interception and transmission of electronic communications for one request criterion	€ 140
Complex requests requiring the intervention of a technical expert	Actual costs

Any operator providing any of the aforementioned services for a request will be reimbursed in accordance with this rate.

5.2 Reimbursements for complex requests

A complex request is to be understood as an exceptional request that is not mentioned under any other section and that exhibits such a verifiable form of complexity that the operator cannot respond to it automatically but only through the intervention of one or more technical experts.

Thus, specific request does not mean the request for provision of services falling within the categories of services with specific rates or services within the flat rate (described hereafter). For these services, operators are deemed to have optimised their operation so that they can quickly provide the requested service or information without the intervention of technicians.

5.3 Annual flat rate

With the aim of facilitating the processing of requests for cooperation and, above all, to simplify the billing of services, all services for which no specific rate of their own fall within the flat rate fee.

The services covered by the flat rate are:

- Identification of a subscriber/user, devices, and/or subscribed services ;

[25] Request criterion = the element or group of elements transmitted by the judicial authorities to an operator with a view to obtaining cooperation (art. 1.b of the annex to the RD 08/11/2016)

- All administrative and technical interventions required in the event of identification, localisation or interception.

Two types of flat rate can be distinguished:

1. € 1.300.000: to be distributed proportionally among operators who handled more than 4% of all requests in the previous year.
2. € 1.000: for the operator who treats less than 4% of all requests per year, who has established a coordination cell and who is (either fully or lightly) integrated with the exchange platform TANK.

6 Lexicon

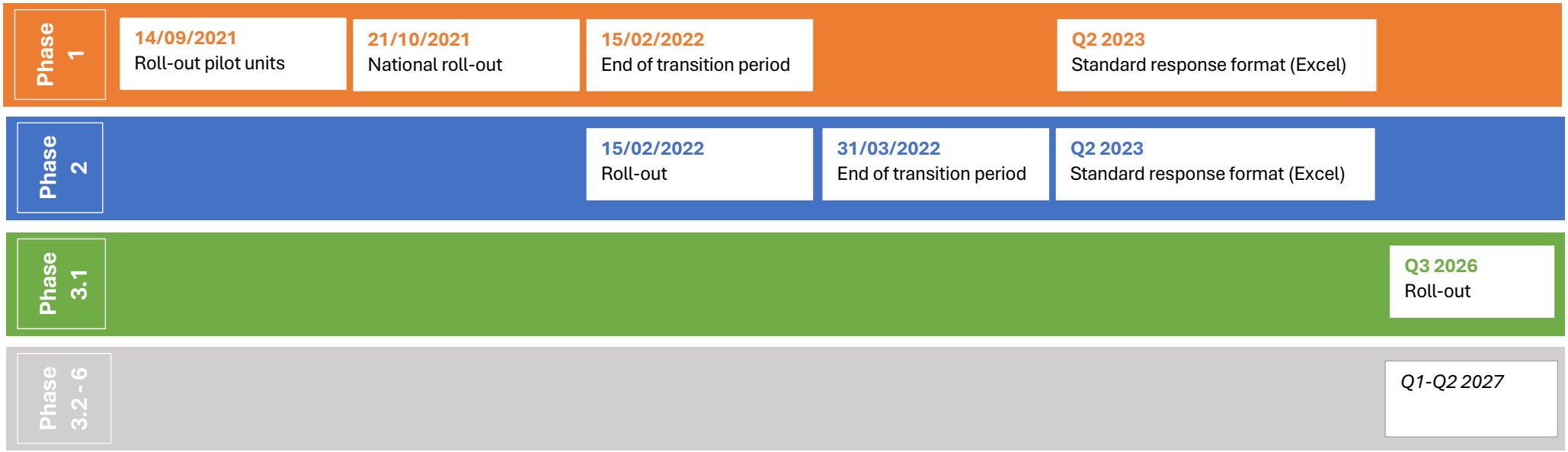
BCA	Belgian Competition Authority
BIPT	Belgian Institute for Postal Services and Telecommunications
CC	Coordination Cell
CCB	Centre for Cyber security Belgium
CCP	Code of Criminal Procedure
CGI	Cell Global Identifier
COC	Supervisory Body for Police Information
CTIF	Central Technical Interception Facility
DEX	Daily execution
DSA	Digital Services Act
DSL	Digital subscriber line
e-Evidence Directive	Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings
e-Evidence Regulation	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
eSIM	Embedded-SIM
ETSI	European Telecommunications Standards Institute
FPS	Federal Public Service
FSMA	Financial Services and Markets Authority
FTP server	File Transfer Protocol server
GFA	General Functional Administrator
HIS	History
ICC ID	Integrated Circuit Card Identification number

IDN	Identification
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP address	Internet Protocol address
LEC	Law on Electronic Communications
MAC address	Media Access Control address
MD	Ministerial Decree
MMS	Multimedia Messaging Service
MNO	Mobile Network Operator
MSISDN	Mobile Station International Subscriber Directory Number
MVNO	Mobile Virtual Network Operator
NIS2 Directive	Network and Information Security Directive
NTSU	National Technical & Tactical Support Unit
OBN	Observation
OSP	Online Service Providers
PEI	Permanent Equipment Identifier
PSTN	Public Switched Telephone Network
PUK	PIN Unlock Key
RD	Royal Decree
SGRS	Intelligence and Security Service
SMS	Short Message Service
SPOC	Single Point of Contact
SRV	Service
SSID	Service Set IDentifier
SUCI	SUbscriber Concealed Identifier

SUPI	SUbscription Permanent Identifier
TANK	Telecom Automation National Knowledge centre
TAP	Interception
TRK	Track
VLOP	Very Large Online Platforms
VLOSE	Very Large Online Search Engines
VSSE	State Security
XLS	File extension associated with Microsoft Excel
XML	Extensible Markup Language

Annex 1 – TANK development schedule

Please be advised that this schedule is subject to change.



Phase	Use case code	Types of requests	Schedule
1	IDN-01 TRK-01 TRK-02	Identification MSISDN Track MSISDN > IMEI Track IMEI > IMSI / MSISDN	• Roll-out pilot units: 14/09/2021 • National roll-out: 21/10/2021 • End of transition period: 15/02/2022 • Standard response format (Excel): 2023, Q2
2	IDN-03 IDN-06 TRK-03	Identification ICCID Identification IMSI Track IMSI > IMEI	• Roll-out: 15/02/2022 • End of transition period: 31/03/2022 • Standard response format (Excel): 2023, Q2
3.1	HIS-01 HIS-02 HIS-03 DEX-01 DEX-02 DEX-03	History MSISDN History IMEI History IMSI Daily Execution MSISDN Daily Execution IMEI Daily Execution IMSI	• 2026, Q3
4.1	SRV-01 SRV-02 SRV-03 SRV-04 EXT-01	Service MSISDN Service PERSON Service COMPANY Service ADRESS Extra MSISDN > PUK CODE	• Q1-Q2 2027
3.2	HIS-04 HIS-14 HIS-05	History LOCATION History TRAJECT History CGI (CELL ID)	• Q1-Q2 2027

4.2	HIS-07 EXT-02 EXT-03 EXT-04	MSISDN > Copy INVOICE Extra MSISDN > Copy Contract Extra MSISDN > Payment information Extra COVERAGE MAP	• Q1-Q2 2027
5	OBN-01 OBN-02 OBN-03 TAP-01 TAP-02 TAP-03	Observation MSISDN Observation IMEI Observation USER ACCOUNT Interception MSISDN Interception IMEI Interception USER ACCOUNT	• Q1-Q2 2027
6	HIS-06 DEX-04 IDN-02 IDN-04 IDN-05	History IP ADRESS Daily Execution IP ADRESS Identification IP ADRESS Identification MAC ADRESS Identification SSID	• Q1-Q2 2027

Annex 2 – Technical legal specifications

1. Identification data

TYPE OF SERVICE	DURATION	ARTICLES	TYPE OF REQUEST	REMARKS
IDENTIFICATION DATA				
Surname, first name	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 1° + §2, al. 1	IDN	-
Customer details provided when subscribing to the service:				
Date + place of birth	According to the geographical zone	art. 127, §7, al. 2, 3° + §10, 3°	IDN	In case of in registration with a authentication document other than a Belgian electronic ID card or in case of an online payment
Nationality	According to the geographical zone	art 127, § 7, al. 2, 2°	IDN	In case of in registration with a authentication document other than a Belgian electronic ID card
National registry number	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 1° + §2, al. 1	IDN	If registered with operator
Authentication (identification) document + type	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 127, §6, al. 4	IDN	If registered with operator
Issuing Country	According to the geographical zone	art. 127, § 7, al. 2, 5°	IDN	In case of in registration with a authentication document other than a Belgian electronic ID card
Name of company	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 1° + §2, al. 1	IDN	If registered with operator
Address	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 3° + §2, al. 1	IDN	If registered with operator
Email address	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 3° + §2, al. 1	IDN	If registered with operator

TYPE OF SERVICE	DURATION	ARTICLES	TYPE OF REQUEST	REMARKS
TECHNICAL DETAILS				
CGI	According to the geographical zone	Art. 126/2, §2, 6°	HIS	-
MSISDN	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 10° + §2, al. 1	IDN – HIS – Track	-
IMEI	12 months after the end of the session	art. 126, §1, 16° + §2, al. 2	HIS – Track	-
IMSI	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §2, al. 1	IDN – HIS – Track	-
SUPI	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §2, al. 1	IDN – HIS – Track	-
SUCI	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §2, al. 1	IDN – HIS – Track	-
PEI	12 months after the end of the session	art. 126, §2, al. 2	IDN – HIS – Track	-
MAC address	12 months after the end of the session (can be reduced to 6 months after the end of the session)	art. 126, §1, 16°, 3e- + §2 , al. 2-3	IDN	The retention period is reduced to 6 months after the end of the session when the operator keeps other data as referred to in §1, al. 1, 16°
MSISDN of addressee	According to the geographical zone	art. 126/2, §2, 2°	HIS	If suspect and addressee are part of same operator
IMSI of addressee	According to the geographical zone	art. 126/2, §2, 2°	HIS	If suspect and addressee are part of same operator
IMEI of addressee	According to the geographical zone	art. 126/2, §2, 2°	HIS	If suspect and addressee are part of same operator
Start and end time of communication	According to the geographical zone	art. 126/2, §2, 5°	HIS	-

TYPE OF SERVICE	DURATION	ARTICLES	TYPE OF REQUEST	REMARKS
TECHNICAL DETAILS				
Duration of communication	According to the geographical zone	Art. 126/2, §2, 5°	HIS	-
Start and end time of activity on network	According to the geographical zone	art. 126/1, §3, al. 4	Track	Signaling data
Download volume	According to the geographical zone	Art. 126/2, §2, 7°	HIS	In case of data
IP address :				
IP address used for subscription or activation	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 4°, 3e- + § 2, al. 1	IDN	-
IP address of the connection source	12 months after the end of the session	art. 126, §1, 15° + § 2, al. 2	IDN – HIS	-
In case of shared use of an IP address, the ports allocated to it	12 months after the end of the session	art. 126, §1, 15° + § 2, al. 2	HIS	-
First and last access point IP address	12 months after the end of the session	art. 126, §1, 15° + § 2, al. 2	HIS	In case of data
Access point name	12 months after the end of the session	art. 126, §1, 15° + § 2, al. 2	HIS	In case of data

TYPE OF SERVICE	DURATION	ARTICLES	TYPE OF REQUEST	REMARKS
IDENTIFICATION OF SERVICES				
Provider ID + name	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 7° + §2, al. 1	IDN	-
Redirected provider ID + name	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 9° + §2, al. 1	IDN	In case of subalocation
Subscription	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 7° + §2, al. 1	IDN	-
Subscription type	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 7° + §2, al. 1	IDN	-
Start and end of subscription	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 8° + §2, al. 1	IDN	-
Line status	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 7° + §2, al. 1	IDN	Comments on subscription (e.g. Line interrupted)
Call attempts without result	According to the geographical zone	art. 126/1, §3, al. 1		-
Call forwarding or transfer	According to the geographical zone	art. 126/2, §2, 4°		-
Redirected number	According to the geographical zone	art. 126/2, §2, 4°	IDN	In case a call was forwarded to a different number

TYPE OF SERVICE	DURATION	ARTICLES	TYPE OF REQUEST	REMARKS
PAYMENT DATA				
The billing address for the service, type and method of payment, date of payments, and reference of the payment transaction in the case of online payment	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 6° + §2, al. 1		-
For online payments : the payment transaction reference, surname/first name, address and date of birth	According to the geographical zone	art. 127, §10, 3°		-
Traffic data solely for invoicing	Data processing is only authorised until the end of the period during which the invoice may be contested or until the end of the period during which action may be taken to obtain payment.	art. 122, §2, al. 3		-

2. Traffic data and network connection

		TYPE OF DATA	REMARKS	PERIOD OF RETENTION	ARTICLES	PHONE	
						Mobile	Fixed line
TRAFFIC DATA	Outgoing communication (Voice/SMS and PSTN)	MSISDN addressee	In mandate asked to identify all contacted persons	According to the geographical zone	art. 126/2, §2, 2°	☑	☑
		Date, hour	-	According to the geographical zone	art. 126/2, §2, 5°	☑	☑
		Location pylon	-	According to the geographical zone	art. 126/2, §2, 9°	☑	
		Start-/end time	-	According to the geographical zone	art. 126/2, §2, 5°	☑	
		Name provider	-	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 7° + §2, al. 1	☑	☑
		IMSI	We do not automatically receive the IMSI of the person contacted by the suspect.	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 12° + §2, al. 1	☑	
		IMEI + type/brand of device	We do not automatically receive the IMEI of the person contacted by the suspect. Possibly if both numbers are with the same operator, must be specifically asked.	12 months after the end of the session	art. 126, §1, 16° + §2, al. 2	☑	
		(e)(raw)CGI	-	According to the geographical zone	art. 126/2, §2, 6°	☑	☑
		Technology used	4G, 5G	According to the geographical zone	art. 126/2, §2, 1°	☑	☑
		Type technology	Volte, voip, vowifi	According to the geographical zone	art. 126/2, §2, 1°	☑	☑

		Antenna	Height, grade, type	According to the geographical zone	art. 126/2, §2, 6°	☑	☑
	Incoming communication (Voice/SMS and PSTN)	MSISDN (at the origin of the incoming call)	The mandate will most likely ask to also identify all contacted persons	12 months from the date of the communication	art. 122, §4, 2°, 1st -	☑	☑
	Data (5G included)	Date, time	-		art. 126/2, §2, 5°	☑	☑
		IMEI	-	12 months after the end of the session	art. 126, §1, 16° + §2, al. 2	☑	☑
		SUCI/SUPI/…	-	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 13° to 14° + §2, 1er	☑	
		IMSI	-	For as long as the electronic communications service is in use and for 12 months after the end of the service	art. 126, §1, 12° + §2, 1er	☑	☑
		Protocol	IRI, Extend evidence, HTTPS, …	According to the geographical zone	art. 126/2, §2, 1°	☑	☑
		Volume of data	-	According to the geographical zone	art. 126/2, §2, 7°	☑	☑
		MAC address	-	12 months after the end of the session / Can be reduced to 6 months after the end of the session (with condition)	art. 126, §1, 16°, 3e tiret + §2 , al. 2-3	☑	☑
		Data types	= "technische karakteristieken"	According to the geographical zone	art. 126/2, § 2, 1°	☑	☑
		IP address (when making a data call)	Possibly through PCAP analysis	12 months after the end of the session	art. 126, §1, 15° + §2, al. 2	☑	

	TYPE OF DATA	REMARKS	PERIOD OF RETENTION	ARTICLES	PHONE	
					Mobile	Fixed line
NETWORK CONNECTION	Switch on equipment	The date and time of connection of the terminal equipment to the network as a result of that equipment being switched on	6 months after being generated or treated	art. 126/2, §2, 8° + §2, al. 2	☑	
	Switch off equipment	The date and time of disconnection of that terminal equipment from the network as a result of that equipment being switched off	6 months after being generated or treated	art. 126/2, §2, 8° + §2, al. 2	☑	
	Activity on network	a.k.a. signalling data	According to the geographical zone	art. 126/1, §3, al. 4	☑	

Annex 3 – Other documents

Upon integration with the exchange platform TANK, the operator receives the Terms and Conditions document, which functions as a contract between the operator and the NTSU and a Parameter Definition Document, which contains more information and details regarding the technical background of the requests.