Telenet Group NV/SA
Law Enforcement Disclosure Report
2022 Report (March 2023)

Contents

Executive summary

This report on the legal obligations for network operators and providers of electronic communication services aims to offer insights into the context and extent of surveillance and collection requests regarding customer data initiated by the Belgian government and authorities at Telenet Group NV. The report includes statistics on conventional (day-to-day) authority requests and information on legislation regarding mandatory 'data retention' for law enforcement purposes. This report is published on the Telenet Group NV corporate website in the section Sustainability Reporting.

Telenet is obliged to report on these statistics towards the Belgian telecom regulator BIPT (Belgian Institute for Postal Services and Telecommunication). The same information can be found below.

1. Statistics

1.1. Statistics regarding requests for subscription, usage and content data

Scope: All warrants and requests by the judicial authorities in execution of the Law on Electronic Communications of 13 June 2005This regards insights into subscription, usage and content (legal intercept) data.

Requests received:

Total received Warrants in 2022

- Total numbers of Warrants received **=56.389 of which 4.538** for **LYCA Mobile and 190 for VOO FMVNO and 20.943 via TANK**

- Warrants can contain multiple requests related to multiple individuals. Below an overview on total received requests split by age category and authority

Requisitioner	Period between data storage and data request					Cases where requests for data could not be met
	# < 3 months	3 months =< # < 6 months	6 months =< # < 9 months	9 months =< # < 12 months	12 months < #	
Justice	56.522	6.884	3.641	291.122	40.201	646
Emergency Services	685	0	0	0	0	0
Mediation Service for Telecommunications	671	60	12	10	295	10
Intelligence and Security Services	1.109	284	170	322	9.483	23
Officers of the judicial police of the Institute	0	0	0	0	0	0
Cell missing persons	0	0	0	0	0	0
FSMA	0	0	0	0	0	0

During 2022 VOO has decided to split their mobile customers over 2 RANs in Belgium (Telenet Group NV and Proximus) therefore the expected growth in warrants for VOO (incl. interceptions) was not maintained.

Lyca Mobile/VOO Full MVNO-actions cannot be split out through the requestor, but we can state that between 1/1/2022 -31/12/2022 for LYCA Mobile => **7.626** actions – or **8.151** **individual targets** were executed. for VOO Mobile **285** actions for **451** individual targets.

.

1.2. Statistics on identification requests, IMEI- and location tracking

Scope: Requests to receive data on identification, IMEI-tracking, Reload info, IP-addresses, and location-tracking (called online tracking). These are all individual requests.

Requests received:

2022 TLNG	
IDENTIFICATIONS	
IDF ADDRESS	631
IDF COMP	168
IDF IMSI	68
IDF IMSDN	25
IDF MEDIATION	636
IDF MSISDN	198.319
IDF NADOB	4.065
IDF NAME	519
TOTAL	**204.431**
IMEI TRK	
IMEI TRK	**12.780**
Reload information	
TOP UP MSISDN	174
TRK SERIE	7
TRK SCR	9
BAL_MSISDN	89
Total	**279**
IP	
IDF	7.355
IP LOG	928
Total	**8.283**
Online tracking	
TRACING	489
Site map	329
Total	**818**
Grand total	**226.591**

2022 LYCA	
Identifications	N/A
IMEI TRK	47
Herlaadgegevens	N/A
IP adressen	N/A
Online Tracking	42

2022 VOO	
Identifications	N/A
IMEI TRK	1
Herlaadgegevens	N/A
IP adressen	N/A
Online Tracking	9

This figure is far below last years due to the impact of TANK implementation and success.

1.3. Tank Requests

Tank rollout went slower than expected due to capacity and delay on the Fed Pol side however we can state that the project for now is a success. 78% of the services which are possible in TANK are executed by this new channel. In total at end of 2022 almost 47% of the total requests were handled without any human interaction (with exception of the audit controls on the requests – spot check if the requests are valid).

TANK REQUESTS (Full Automatic)	JAN	FEB	MRT	APR	MEI	JUNI	JULI	AUG	SEP	OCT	NOV	DEC	2022
IDF-01 - MSISDN (09/21)	1.050	1.070	1.323	1.021	1.303	1.043	1.010	1.139	1.192	1064	1133	1.123	13.471
IDN-03 (14/02/22) ICCD		2	14	0	2	6	3	11	9	7	6	13	73
IDN-06 (14/02/22) - IMSI		6	14	2	5	2	1	5	4	6	3	3	51
TRK-01 MSISDN (09/21)	133	148	175	163	189	149	140	150	141	142	136	140	1.806
TRK-02 IMEI (09/21)	344	409	486	256	665	424	387	459	526	499	415	481	5.351
TRK-03 (14/02/22) - IMSI		15	26	12	11	5	9	11	14	8	11	12	134
HIS-01								7		4		10	21
HIS-02								7		1		11	19
HIS-03								7				10	17
SRV-01													0
SRV-02													0
SRV-03													0
Total	1.527	1.650	2.038	1.454	2.175	1.629	1.550	1.796	1.886	1.781	1.704	1.803	20.943

2. Legal framework

1.1. Introduction

The legal framework that regulates the cooperation of an operator of a network or the electronic communications service provider with the government is formed by a series of articles spread across various Acts and Royal Decrees (RD). Below you will find an overview of the most important articles in these Acts and Royal Decrees with a brief description of the content and the competent government. An in-depth reading of these articles is necessary for operators and service providers to be able to estimate their full scope. This overview is limited to the cooperation with judicial authorities and intelligence services. Other authorities (e.g. tax inspection) also have powers to question operators and service providers, but this document does not go further in detail regarding these authorities.

Update 2023: Following the annulment of the previous data retention law by the Constitutional Court, a new data retention legislation was published in August 2022 which invokes changes.

1.2. Basic provisions: respect for privacy and secrecy of communications

The protection of the personal and family life of each person is guaranteed by Article 22 of the Constitution and Article 8 of the ECHR (European Convention on Human Rights). Any deviation from this is only possible if foreseen by law. The Belgian Criminal Law states in Articles 259bis and 314bis that the interception of private communications is punishable. These articles also stipulate that the usage of equipment to intercept such communications as well as the use or trading of information obtained from illegal interception are deemed illegal. The Law Electronic Communications of 13 June 2005 (LEA) further elaborates on the protection of electronic communications, and states that it is forbidden to learn about the existence of electronic communications, identity and location of the

parties involved and of the content of these communications. It is forbidden to keep track of these communications unless they have been anonymized or in certain cases consent was obtained. The LEA also determines the cases and circumstances in which the above-mentioned legal principles can be waived. The LEA determines which electronic communications data should be kept and lists the authorities who can retrieve this information. The Code of Criminal Procedure and the Security and Intelligence Act provide the powers and circumstances under which competent authorities may request electronic communications information, intercept electronic communications, or ask the cooperation of an operator or service provider. These Acts require operators or service providers to cooperate with the prosecuting authorities.

1.3. Code of criminal procedure

Below you can find the main articles on data retention and which entity can requests the retrieval of the data.

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

LOI - WET (fgov.be) : for investigations and judicial investigations

LOI - WET (fgov.be): for criminal investigations

1.4. Royal Decree establishing the obligation to cooperate in court proceedings

RD January 2003: Terms and provisioning for the legal obligation to cooperate in legal warrants relating to electronic communications, hereby you can find the main and relevant articles out of this RD .

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

LOI - WET (fgov.be)

1.5. Intelligence Services Act

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

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

LOI - WET (fgov.be)

1.6. Duty to collaborate with warrants provided by the intelligence services

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

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

LOI - WET (fgov.be)

1.7. Law on Electronic Communications (LEA) of 13 June 2005

Art.	Description
122	Basic principle to delete or anonymize the traffic data, but exceptions apply: - Invoicing - Marketing purposes - To combat fraud or malicious use of the network - Security purposes
123	Clarifies under which conditions operators can keep and process other location data than traffic data.
124	General principle of secrecy of communication: prohibition of notice, identification, interception and use of this information
125	Exceptions to Article 124
126	determines which identification data operators must keep (to the extent processed or generated by the operator).
126/2, §2	Determines the meta data which must be stored by the operators
127/1	Overview of the authorities which can receive information from the operators
127/2, §1, §2 and §3	quality requirements for storing the data. The operators can only store the data in the EU. Operators must keep a logbook and any consultation of the data should be logged.
127/3, §1 and §2	rules with respect to the Coordination Cel

LOI - WET (fgov.be)

1.8. Royal Decree on retention of data

RD concerning execution of Article 126 of the Act of 13 June 2005 on electronic communications (13/09/2013)

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

LOI - WET (fgov.be)

1.9. RD Regarding the identification of users of prepaid cards

RD regarding identification of end-user of public electronic mobile communications services provided by a prepaid card (27/11/2016).

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

Telenetgroup has implemented in December 2021 an MRZ capable customer onboarding and fall out (for documents not readable with e-reader or MRZ can be followed up). BIPT agreed to the solution.

1.10. MD on buffering and filtering of electronic communications

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

- The instalment of a buffer capacity by the operators to ensure that in the event of a connection failure between operator and NTSU CTIF, no data will be lost
- Filtering possibilities that an operator has to provide before the data reaches NTSU CTIF. Objective of this filtering is to limit the amount of electronic intercepted data to the strict minimum as requested by the investigating judge. MB published 05/08/2020.

Telenetgroup is compliant however testing with CTIF has still to be planned by them.

2022 no change in the situation for the moment still awaiting interaction with CTIF on the testing (planned interaction 03/2023)

Moniteur Belge - Belgisch Staatsblad (fgov.be)