ОБЕЗБЕДУВАЊЕ ДОКАЗИ ВО ЕЛЕКТРОНСКА ФОРМА ОД МЕЃУНАРОДНИ И ДОМАШНИ ИНТЕРНЕТ СЕРВИС ПРОВАЈДЕРИ

КРАТОК ВОДИЧ ЗА ОБВИНИТЕЛИ

јуни, 2017

Автори:

м-р Марјан Стоилковски, *Началник на Сектор за компјутерски криминал и дигитална форензика при МВР*

м-р Јован Цветановски, *Јавен обвинител во Вишото јавно обвинителство Скопје*

Уредник и соработник:

Ана Новакова-Жикова, *Национален офицер за владеење на правото при Мисијата на ОБСЕ во Скопје*

Тираж: 1000 примероци

Печати: Европа 92, Кочани

ОБСЕ Организација за безбедност и соработка во Европа
Мисија во Скопје

Содржината на ова издание не секогаш ги одразува погледите или ставовите на Мисијата на ОБСЕ во Скопје. Мисијата се придржува до Одлуката PC.DEC/81 на Постојаниот совет на ОБСЕ.

СОДРЖИНА

Вовед 5

1. КРАТОК ПРЕГЛЕД НА ДОМАШНАТА И МЕЃУНАРОДНАТА ПРАВНА РАМКА 6

2. МЕЃУНАРОДНА ПОЛИЦИСКА СОРАБОТКА И МЕЃУНАРОДНА ПРАВНА ПОМОШ 6

3. ШТО ТРЕБА ДА СЕ ПОБАРА КАКО КОМПЈУТЕРСКИ ПОДАТОК ОД ПРОВАЈДЕРОТ 8

3.1 Што претставува интернет сервис провајдер и какви услуги нуди 8

3.2 Какви податоци можат да се обезбедат од интернет провајдерите 10

4. ПОЛИТИКИ И ПРОТОКОЛИ ЗА ОБЕЗБЕДУВАЊЕ НА КОМПЈУТЕРСКИ ПОДАТОЦИ ОД СТРАНА НА ДОМАШНИ И СТРАНСКИ ПРОВАЈДЕРИ 19

4.1 Домашни интернет провајдери 19

4.2 Странски интернет провајдери 21

4.3 Соработка со странски интернет провајдери од кои најчесто се обезбедуваат компјутерски податоци 26

4.4. Видови достапни податоци и услови за нивно доставување 31

4.5 Итни барања за зачувување на податоците 33

4.6 Постапки за испраќање на барања во итни случаи 34

4.7 Зачувување на податоци 35

5. НАМЕСТО ЗАКЛУЧОК 41

ПРИЛОГ 1: Листа на адреси на интернет сервис провајдери 42

Вовед

Водичот што го имате пред Вас, почитувани колеги, има за цел да Ви ја олесни работата во случаите кога е потребно да се обезбедат компјутерски податоци кои подоцна би се користеле како потенцијален доказ во кривичната постапка. Водичот опфаќа неколку аспекти, кои веруваме би биле од корист при практичното постапување на обвинителите, полициските службеници, но и на другите учесници во кривичната постапка:

- Дефинирање на компјутерските податоци кои можат да им бидат потребни на правосудните органи во текот на кривичната постапка;
- Преглед и информации за видот на компјутерските податоци кои може да се добијат, каде се наоѓаат и како можат да бидат обезбедени во текот на претходната постапка, согласно домашната и меѓународната правна рамка;
- Начинот и постапката кои треба да се следат при обезбедување на компјутерските податоци кои би можеле да бидат потенцијален доказ во постапката;
- Обрасци за поднесување барања за податоци од домашни или странски интернет провајдери.

Водичот е изготвен во насока на олеснување и воедначување на практичното постапување на обвинителите и полициските службеници при обезбедување на потенцијални докази од електронска природа. Се надеваме дека ќе даде свој придонес во надминување на постојниот проблем со недостаток од информации за компјутерски податоци и дека ќе биде корисна и практична алатка при постапување со вакви предмети.

1. КРАТОК ПРЕГЛЕД НА ДОМАШНАТА И МЕЃУНАРОДНАТА ПРАВНА РАМКА

Во процесот на обезбедување на компјутерски податоци кои би можеле во конкретен случај да претставуваат доказ во кривичната постапка, потребно е да се следи како домашната така и меѓународната регулатива, ратификувана од нашата држава. Краткиот преглед подолу ги посочува клучните домашни закони и меѓународни документи кои треба да се следат во овие постапки:

➢ *Домашна правна рамка*

- Закон за кривичната постапка
- Кривичен законик
- Закон за меѓународна соработка во кривичната материја
- Закон за следење на комуникациите

➢ *Меѓународни документи*

- Европска конвенција за компјутерски криминал ETC 185
- Европска конвенција за меѓусебна правна помош во кривичната материја ETC 030
- Европска спогодба за пренос на барањата за правна помош ETC 092

2. МЕЃУНАРОДНА ПОЛИЦИСКА СОРАБОТКА И МЕЃУНАРОДНА ПРАВНА ПОМОШ[1]

➢ *Меѓународна полициска соработка*

Меѓународна полициска соработка е инструмент кој го користат полициските службеници согласно овластувањата кои се дефинирани во Законот за полиција. Овој инструмент полици-

[1] Ова поглавје нема за цел да ги образложи во целост постапките за меѓународна полициска соработка и меѓународна правна помош, туку само накратко ја сумира целта на овие инструменти во процесот на обезбедување на компјутерски податоци како потенцијални докази во кривичната постапка.

ските службеници го користат за размена на полициски информации за истраги и лица кои се или биле предмет на истрага во нашата држава. Преку овој инструмент на полицијата можат да се разменуваат и други податоци со кои располагаат полициските служби.

Разменетите податоци преку инструментот на меѓународна полициска соработка можат да се користат исклучиво за полициска намена, но никогаш како доказ во истражната постапка.

Преку меѓународна полициска соработка можат да бидат испраќани информации до полициските служби на други држави за отпочната постапка за меѓународна правна помош, но никогаш овој полициски инструмент не може да биде замена за постапката за меѓународна правна помош која е во надлежност на јавниот обвинител.

➢ *Меѓународна правна помош*

Суверените држави отсекогаш требале да доставуваат барања до други суверени држави во врска со прибирање докази за кривични дела кои содржат меѓународен елемент. Во тие случаи може да се достави барање за меѓународна правна помош или да се побара друга форма на соработка. Преку-граничните барања за помош се особено важни кога треба да се обезбедат електронски докази бидејќи постои ризик овие докази да се изменат или избришат. Вистинскиот предизвик во таквите случаи е да може да се делува доволно брзо со цел навремено да се обезбедат доказите.

Кога се поднесува барање за меѓународна правна помош, потребно е обвинителствата, или понекогаш судските органи, да поднесат формално барање. Но, успешноста на таквите барања често пати зависи од подготвеноста и нивото на стручност на учесниците, како кај органот барател, така и кај органот од кој податоците се побарани. Покрај тоа, за да се комплетира барањето може да биде потребно одредено време.

Подолу на сликата 1 е претставен еден предлог образец за доставување на известување до Министерството за правда дека јавното обвинителство испратило барање за меѓународна правна помош.

ОСНОВНО ЈАВНО ОБВИНИТЕЛСТВО
РО бр.
Скопје, 2017 година

ДО
МИНИСТЕРСТВО ЗА ПРАВДА
СЕКТОР ЗА МЕЃУНАРОДНА СОРАБОТКА

С К О П Ј Е

ПРЕДМЕТ: Известување за испратено барање за меѓународна правна помош

Во врска со оформениот предмет РО бр........../17 во Основното јавно обвинителство Скопје, во текот на кривичната постапка за прибирање на докази кои се однесуваат на стореното кривично дело, согласно член 6 ст.4 и 6 од Законот за меѓународна соработка во кривичната материја, Ве известувам за поднесено барање за меѓународна правна помош до одговорното лице од *„име на интернет сервис провајдер*". Барање за зачувување податоци е испратено преку Секторот за компјутерски криминал и дигитална форензика при МВР и провајдерот има отворено случај со број.....

Во прилог Ви се доставува примерок од испратените барања, заради Ваше запознавање и известување.

ЈАВЕН ОБВИНИТЕЛ

Слика 1

3. ШТО ТРЕБА ДА СЕ ПОБАРА КАКО КОМПЈУТЕРСКИ ПОДАТОК ОД ПРОВАЈДЕРОТ

3.1 Што претставува интернет сервис провајдер и какви услуги нуди

Интернет сервис провајдери (ISP), за прв пат почнаа да се појавуваат кон крајот на 1980-тите и раните 1990-ти. Тоа се приватни компании кои им обезбедуваат на корисниците интернет пристап и услуги преку интернет. Овие провајдери овозможуваат

поврзување на клиентите во интернет мрежа и пристап на сервисите на интернет мрежата. Често пати, интернет провајдери се компании кои нудат телекомуникациски услуги, вклучувајќи интернет комуникација, пристап до податоци и телефонска врска. Поголемиот дел од телефонските компании сега функционираат како интернет-провајдери, кои може да бидат комерцијални, непрофитни, приватни или со заедничка сопственост.

Некои од услугите на интернет провајдерите вклучуваат интернет пристап, регистрација на домејн, име на домејн хостинг, dial-up пристап, пристап на изнајмена линија и ко-локација. Генерално, интернетот е глобален систем на меѓусебно поврзани компјутерски мрежи кои се користат од страна на милијарди луѓе од целиот свет. Овој систем на мрежи е поврзан со огромен асортиман на електронски, оптички мрежи и безжични технологии.

Постојат неколку различни видови на интернет сервис провајдери во зависност од услугата што ја нудат, односно дали станува збор за интернет пристап, електронска пошта, хостирање на интернет сервис, информативен сервис, социјални мрежи и останати сервиси на интернет мрежата.

Провајдерите на интернет конекција своите услуги ги нудат преку технологии кои обезбедуваат интернет конекција. Интернет конекцијата или интернет пристапот може да биде овозможен преку кабел, оптичка (FiOS), DSL (Digital Subscriber Line) или сателит. Голем број провајдери на интернет пристап, исто така обезбедуваат e-mail и дополнителни услуги за хостирање на одредени услуги.

Интернет провајдери кои нудат e-mail услуги или хостинг услуги на e-mail сервери всушност нудат сервис за испраќање, примање и чување на e-mail пораки. Голем број на e-mail провајдери се и провајдери на други услуги на интернет.

Хостинг провајдерите нудат сервис на интернет за e-mail, пренос на датотеки преку FTP протокол, веб-хостинг услуги, виртуелни машини, Cloud и физички сервери.

Трансфер интернет провајдерите овозможуваат услуги на интернет кои нудат големи количини на пропусен опсег потребен за меѓусебно поврзување на хостинг провајдерите и интернет провајдерите.

Виртуелните интернет провајдери (Visp) нудат набавка на услуги од други интернет провајдери со цел да им овозможат на корисниците пристап до интернет.

Бесплатните интернет провајдери (freenets) даваат бесплатна услуга за пристап до интернет и често се прикажуваат реклами додека корисниците се поврзани.

3.2 Какви податоци можат да се обезбедат од интернет провајдерите

Голем дел од истрагите кои тековно се водат имаат потреба од компјутерски податоци кои ги поседуваат интернет сервис провајдерите во нашата и во други држави. Во текот на претходната постапка обезбедувањето на потребните компјутерски податоци може да биде неизвесно и во случаите каде правосудните органи кои се задолжени за водење на истрагите веќе отпочнале постапка за обезбедување на компјутерските податоци и во оние случаи каде таа постапка сѐ уште не е започната. Неизвесноста произлегува од следново:

а) Кај започната постапка за обезбедување компјутерски податоци јавниот обвинител и полицијата:

- не се сигурни дали бараните податоци постојат,
- дали истите ќе бидат дадени врз основа на отпочнатата постапка, и
- кој е реалниот временски рок во кој може да се очекува декаќе бидат доставени бараните податоци.

б) Кај одреден број случаи јавниот обвинител и полицијата не отпочнале постапка за обезбедување на компјутерски податоци бидејќи:

- немале точни информации за тоа дали тие податоци воопшто постојат и дали се достапни,
- кој ги поседува податоците и од кого треба истите да бидат побарани, и
- која е постапката да се побараат потребните компјутерски податоци.

Секако дека сето ова влијае на текот на предистражната и истражната постапка бидејќи тековно има случаи кои не се комплетирани бидејќи се чека одговор од интернет провајдерите, иако јавниот обвинител и полицијата не се сигурни дали ќе ги добијат бараните податоци. Истовремено, има и случаи кои не можат ефикасно да се завршат токму затоа што недостасуваат компјутерски податоци кои не биле побарани навремено. Она што треба особено да се посочи е дека:

Ефикасноста во решавањето на предметите за кои е потребно да се обезбедат компјутерски податоци кои би можеле да претставуваат потенцијален доказ во постапката е намалена.

За целите на кривичната истрага, најчесто е потребно да бидат обезбедени следниве видови податоци:

- *"Податоци за претплатникот"* - информации за идентификација на корисникот на одреден Интернет Протокол (IP адреса) или IP адреси кои се користатод страна на одредена личност. Овие податоци претставуваат и дел од податоците кои можат да се добијат од регистрите на регистранти на домени.
- *"Податоци за интернет сообраќај"* - преставуваат log датотеки каде се евидентирани активности на оперативниот систем на одреден компјутерски систем или на друг софтвер или на комуникации помеѓу компјутери, особено на изворот и дестинацијата на пораките.
- *"Податоци за содржина"* – Во овој вид влегуваат пораки, слики, филмови, музика, документи или други податоци. Постои разлика помеѓу содржини кои се чуваат односно податоци кои се веќе достапни на компјутерски систем и содржини кои треба да бидат сочувани во иден период, а кои сѐ уште не се на располагање и ќе мора да бидат добиени во реално време.

Податоците за претплатниците се најчесто барани компјутерски податоци при домашните и меѓународните истраги. Без овие информации, често е невозможно да се отпочне или продолжи со истрагата и затоа е од клучно значење нивното обезбедување. Во групата на овие податоци генерално влегуваат

податоци за кои се смета дека по својата природа се лични и приватни податоци, па затоа секое обезбедување на овие податоци потребно е да биде во согласност со законот. Оттука, повеќето системи имаат воспоставени строги заштитни мерки во однос напристапот, особено кога се работи за обезбедување на податоци кои влегуваат во т.н. "податоци за содржина" (на пример следење на комуникациите).

Податоците за претплатникот обично се процесираат и чуваат од страна на давателите на услуги односно интернет сервис провајдерите кои се дел од приватниот сектор, што значи сите податоци кои се бараат потребно е да бидат со наредба од јавен обвинител. Издавањето на наредби за доставување на податоци често може да биде третирано како загрозување на човековите права и правото на приватност, исто како и пребарувањето и заплената на компјутерски системи или следењето на комуникации. Во овој контекст и Европската конвенција за компјутерски криминал на Советот на Европа прави разлика помеѓу податоци за претплатникот, податоци за интернет сообраќај и податоци за содржината.

Важно:

Само податоците за претплатникот може да бидат побарани директно со наредба. Останатите податоци мора да бидат побарани преку постапката за меѓународна правна помош.

Домашната процесна правна рамка која предвидува различни начини и механизми за обезбедување на информации (на пример: налози за производство, требувања или судски покани за барање на информации од провајдерите на интернет услуги и сл.) не важат во други држави. За да се добијат информации од странски провајдери националните барања треба да одат преку дополнителни правни механизми и постапки како меѓународна правна помош. Прибирањето на електронски докази од странски независни иматели на податоци може да одземе многу време и постои ризик дека додека имателот на информацијата, кој е провајдер на услугата, го добие барањето согласно нивното национално право, бараните податоци може повеќе да не се достапни. Провајдерите на комуникациски услуги, интернет и телефон не чуваат податоци за комуникацискиот сообраќај вечно и честопати таквите податоци не се чуваат подолго од

времето потребно за исполнување на обврските за плаќање или слични обврски.

Подолу во текстот е претставен еден пример за содржината на барање за меѓународна правна помош за обезбедување на комјутерски податоци кои би можеле да бидат потенцијален доказ во одредена кривична постапка. Предлог образецот е даден на англиски јазик во интерес на олеснета комуникација со интернет сервис провајдерот.

REQUEST FOR MUTUAL ASSISTANCE
REGARDING ACCESSING OF STORED COMPUTER DATA

First request: ❒ Yes ❒ No

Ticket number of the previous request (if available): ....

REQUESTED AUTHORITY	
REFERENCE / CASE NUMBER	
REQUESTING AUTHORITY	
DATE	
DD/MM/YYYYY	
SUBJECT/TITLE	
PURPOSE OF THE REQUEST	
URGENCY	
❒**URGENT** Response expected by: DD/MM/YYYY	

REASONS FOR URGENCY
❐Threat to life and limb
❐Offender in custody
❐Crime in progress
❐Imminent threat of a serious nature to public security
❐The only evidence available
❐Volatility of data
❐Statute of limitation due to expire
❐ Other:...
DESCRIPTION/JUSTIFICATION FOR URGENCY

OFFENCES SUBJECT TO CRIMINAL INVESTIGATION OR PROCEEDINGS,

(Irrespective of their consideration in the requested State)

OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND SYSTEMS / COMPUTER-RELATED OFFENCES	
❐	Illegal Access
❐	Illegal Interception
❐	Data Interference
❐	System Interference
❐	Misuse of devices
❐	Computer-related forgery
❐	Computer-related fraud
❐	Offences related to child pornography
❐	Offences related to infringement of copyright and related rights
OTHER OFFENCES SUBJECT TO CRIMINAL INVESTIGATION OR PROCEEDINGS	
❐	Terrorism
❐	Sabotage
❐	Murder
❐	Grievous bodily injury
❐	Kidnapping, illegal restraint and hostage-taking
❐	Racketeering and extortion
❐	Rape/offences against sexual liberty
❐	Sexual exploitation of children and child pornography

❒	Trafficking in human beings
❒	Illicit trade in human organs and tissue
❒	Trafficking in stolen vehicles
❒	Money laundering/Laundering of the proceeds of crime
❒	Fraud
❒	Counterfeiting currency
❒	Forgery of means of payment
❒	Forgery of documents
❒	Counterfeiting and piracy of products
❒	Bribery of national public officials
❒	Bribery of foreign public officials and officials of public international organizations
❒	Embezzlement, misappropriation or other diversion of property by a public official
❒	Trading in influence
❒	Abuse of functions
❒	Illicit enrichment
❒	Bribery in the private sector
❒	Participation in a criminal organization
❒	Organised or armed robbery
❒	Illicit trafficking in narcotic drugs and psychotropic substances
❒	Illicit trafficking in weapons, munitions and explosives
❒	Illicit trafficking in cultural goods, including antiques and works of art
❒	Illicit trafficking in hormonal substances and other growth promoters
❒	Illicit trafficking in nuclear or radioactive materials
❒	Environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties
❒	Facilitation of unauthorized entry and residence
❒	Arson
❒	Unlawful seizure of aircrafts/ships
❒	Racism and xenophobia
❒	Crimes within the jurisdiction of the International Criminal Court
❒	Other offence(s) (please specify):

APPLICABLE SUBSTANTIVE LEGISLATION
Title of Legislation
Relevant Sections
Right to Request Data
Codes of Practice
Relevant Court Decisions/ Confirmation
APPLICABLE PROCEDURAL LEGISLATION TO BE FOLLOWED IN THE OBTAINING OF EVIDENCE
Title of Legislation
Relevant Sections

Right to Request Data
Codes of Practice
Relevant Court Decisions / Confirmation
CASE STATUS
❐Pre-investigative phase ❐Investigate phase ❐Prosecution phase ❐On trial Other details: ....

DESCRIPTION OF INFORMATION REQUESTED

❐ **SUBSCRIBER INFORMATION**			
Period of Interest			
Start Date		End Date	

Data specification		
❐	Subscriber names	
❐	User names	
❐	Screen names, or other identities	
❐	Mailing addresses	
❐	Residential addresses	
❐	Business addresses	
❐	Email addresses	
❐	Telephone numbers, other contact information	
❐	Billing records	
❐	Billing address	
❐	Payment method	
❐	Payment History	
❐	Billing period	
❐	Information about length of service and the types of services the subscriber(s) or customer(s) used	
❐	Any other identifying information, whether such records are in electronic or other form	
❐	Connection logs and records of user activity for the subscriber(s) identified above, including log-in history and records identifying sent and received communications	

❒ All communications stored in the account(s) of the subscriber(s) identified above			
❒ All files that are controlled by user accounts associated with the subscriber(s) identified above			
Name, username and postal address of the holder of the account			
When was the account registered?		DD/MM/YYYY	
Is the account still active?			
❒ USER DATA			
Service ID (Skype, Windows Live, Chat room, etc.)			
Social Networking Service ID (Facebook, etc.)			
IP address used for the initial registration of the account			
IP address used for the last registered access to the account			
IP address used for access to the account on **Date**: DD/MM/YYYY **Time**:			
IP address used for sending message from the account **Message details:** **Date**: DD/MM/YYYY **Time**:			
Other relevant data			
❒ TRAFFIC DATA			
Accessed IP address / range of IP addresses			
IPv4	**1-255**	**1-255**	**1-255**
Date		Time	
Time Zone			
IPv6 Address	**Subnet – 64 bit**	**Host – 64 bit**	
Date		Time	
Time Zone			
E-mail Address Specification			
E-mail address		@	
Date		Time	
Zone Time			

Person/Organisation details	
Business Name	
Legal Name	
Contact name	
Address	
Country	
Phone	
E-mail	

❐ CONTENT DATA	
❐	Electronically stored documents, records, images, graphics, recordings, spreadsheets, databases; calendars, system usage logs, contact manager information, telephone logs, internet usage files
❐	Deleted files, cache files, user information, and other data
❐	Archives, backup anddisaster recovery tapes, discs, drives, cartridges, voicemail and other data
❐	All operating systems, software, applications, hardware, operating manuals, codes, keys and other support information
❐	Other:

Origin of the data (if known)	
Destination of the data (if known)	
Other relevant details	

ACTIONS REQUESTED IN RELATION TO DATA

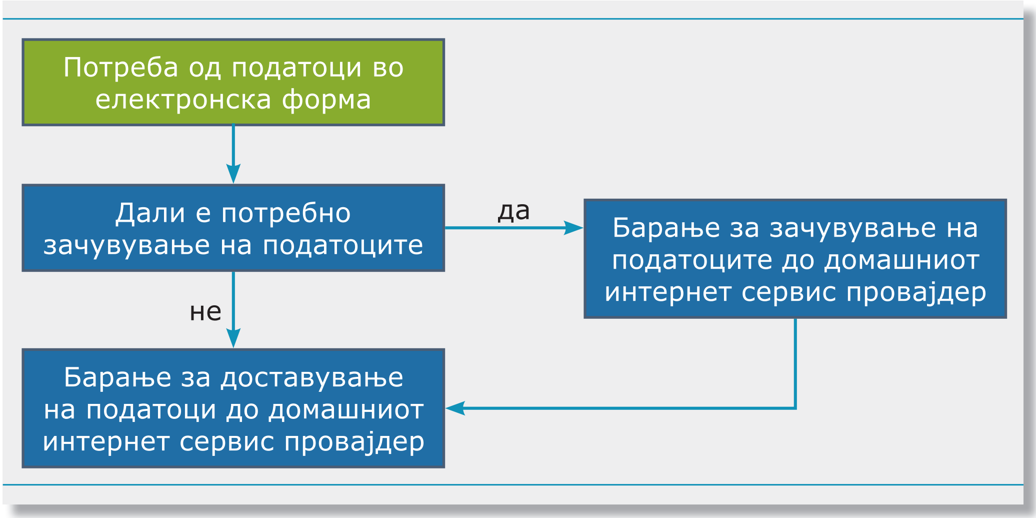
REQUESTING AUTHORITY DETAILS	
Name	
Address	
Telephone number	
Cell phone number	
E-mail address	
Fax number	
Office Hours	
Time Zone	

FOR VERIFICATION BY THE AUTHORISED PERSON, PLEASE CONTACT:	
Name:	
Job Title:	
Function:	
Signature:	

4. ПОЛИТИКИ И ПРОТОКОЛИ ЗА ОБЕЗБЕДУВАЊЕ НА КОМПЈУТЕРСКИ ПОДАТОЦИ ОД СТРАНА НА ДОМАШНИ И СТРАНСКИ ПРОВАЈДЕРИ

4.1 Домашни интернет провајдери

Обезбедувањето на податоци за корисници на интернет сервиси кои се регистрирани во нашата држава е поедноставен процес. Согласно домашната законска регулатива секој провајдер на услуги/сервиси на интернет кој е регистриран во нашата држава има обврска 12 месеци да ги чува податоците за идентификација на корисник. Доколку се работи за податоци за сообраќај и податоци за содржина, потребно е органите за спроведување на законите да упатат Барање за зачувување на податоците до провајдерот на услугата. Подолу на сликата 2 е претставен процесот на поднесување на барање за обезбедување на податоците до домашните интернет провајдери.



Слика 2

При поднесување на барањето за достава компјутерски податоци, јавниот обвинител може директно да се обрати до домашниот интернет сервис провајдер или пак тоа да го стори преку Секторот за компјутерски криминал и дигитална форензика при Министерството за внатрешни работи. На сликата 3 подолу, прет-

ставен е еден предлог-образец за директен контакт на јавниот обвинител со домашниот провајдер. Доколку постапката оди преку Министерството за внатрешни работи (МВР) тогаш јавниот обвинител треба да подготви и наредба (види слика 5 подолу).

ОСНОВНО ЈАВНО ОБВИНИТЕЛСТВО
РО бр.
Скопје, ...година

ДО
Одговорно лице во
„име на интернет сервис провајдер"
Адреса

Врз основа на чл.287 ст.1 и ст.2 од ЗКП, поднесувам

БАРАЊЕ ЗА ДОСТАВА НА ПОДАТОЦИ

Во врска со оформениот предмет РО бр............../...во Основното јавно обвинителство Скопје, по доставеното известување бр................ од .... година на МВР, БЈБ, ЦПС СККДФ, Одделение за истраги за компјутерски криминал, со цел да се добијат сознанија за релевантните факти кои се од суштествено значење при донесување на јавнообвинителска одлука, како интернет провајдер – *„име на интернет сервис провајдер"*, потребно е да доставите комплетни податоци за корисникот на IP адресата 151.258.254.124 на .... година од 17:00 часот до 22:20 часот (локално македонско време).

Бараните податоци потребно е да бидат доставени во најкраток рок, без одлагање.

Бараните податоци сте должни да ги доставите на овластени службени лица од Секторот за компјутерски криминал и дигитална форензика при МВР, при што да се повикате на нивен бр.................. од .... година.

ЈАВЕН ОБВИНИТЕЛ

Слика 3

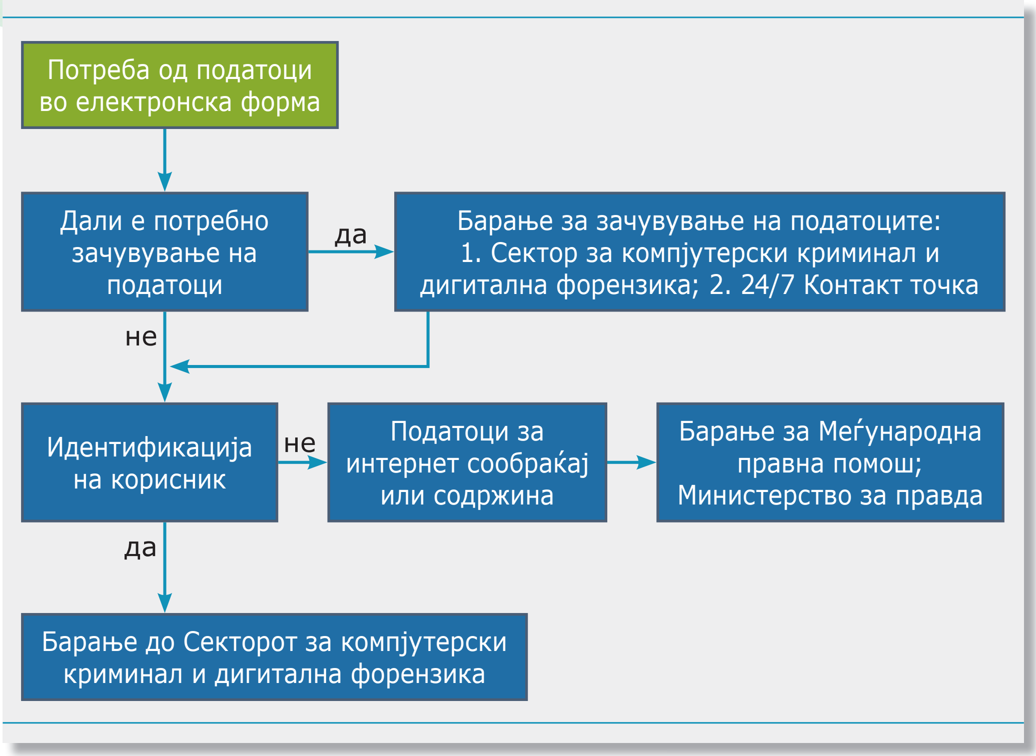
4.2 Странски интернет провајдери

Во текот на истражната постапка се јавува потреба од податоци кои се наоѓаат кај странски интернет сервис провајдери. Процесот на обезбедување на податоците генерално го дефинираат протоколите и постапките на странските интернет сервис провајдери за соработка со органите за спроведување на законот.

Интернет сервис провајдерите кои се регистрирани во САД, согласно актуелната законска регулатива имаат надлежност директно да соработуваат со претставници на органите за спроведување на законот од други држави и истовремено да обезбедуваат податоци за корисниците на нивните интернет сервиси, за корисничките активности, како и за креираните содржини од страна на корисниците на одреден сервис.

Соработката помеѓу овие провајдери и органите за спроведување на законите е на доброволна основа. Позитивно се одговара на оние барања за кои нивните експертски правни тимови сметаат дека треба да бидат обезбедени податоци.

Сликата 4 подолу, го претставува процесот на поднесување на барање за обезбедување на податоци од странски интернет провајдери. Приказот се однесува на една генерална постапка за обезбедување на податоци од меѓународните интернет сервис провајдери, но треба да се има предвид дека секој провајдер поединечно има свои протоколарни особеностите кои се објавени во форма на Процедури за обезбедување на податоци на органите за спроведување на законите.



Слика 4

При поднесување на барањето за достава на компјутерски податоци, јавниот обвинител не може директно да му се обрати на странскиот интернет провајдер, туку е потребно постапката да се спроведе преку Секторот за компјутерски криминал и дигитална форензика при Министерството за внатрешни работи. Во овие случаи барањата треба да се поднесат преку меѓународна правна помош, и јавниот обвинител треба да изготви наредба до МВР и барање за меѓународна правна помош до странскиот интернет провајдер од кој се бараат податоците.

На сликите 5, 6 и 7 подолу како пример дадени се предлог образци за наредбата и барањето (на македонски и англиски јазик).

ОСНОВНО ЈАВНО ОБВИНИТЕЛСТВО
КОН бр.
Скопје, ...година

ДО
МВР, БЈБ ЦПС
Сектор за компјутерски криминал и дигитална форензика,
СКОПЈЕ

Врз основа на чл.283 ст.2 в.в. со чл.284 ст.1 од ЗКП и согласно член 6 ст.4 и 6 од Законот за меѓународна соработка во кривичната материја, ја донесувам следната:

Н А Р Е Д Б А

До Основното јавно обвинителство Скопје од страна на МВР, БЈБ, ЦПС, Центар за полициски служби, Сектор за компјутерски криминал и дигитална форензика под......................................., доставено е барање за добивање податоци од *„име на интернет сервис провајдер*", во врска со пријава од ...., во која се наведува дека од профилот регистриран на *„име на интернет сервис провајдер*" биле упатени индиректни закани кон .... и неговото семејство.

Заради надлежно предметно постапување на ова обвинителство и прибирање на докази во кривичната постапка кои се однесуваат на стореното кривично дело, потребно е од страна на одговорно лице од *„име на интернет сервис провајдер*" да ни бидат доставени следните податоци:

- Логови и ИП адреси од пристапувањето на профилот регистриран на *„име на интернет сервис провајдер*".

Податоците кои се бараат потребно е да содржат точен час, датум, како и временска зона.

Барањето на податоци се спроведува преку Министерството за правда.

Во прилог Ви доставуваме Барање за меѓународна правна помош упатено до *„име на интернет сервис провајдер*", на македонски и англиски јазик.

ЈАВЕН ОБВИНИТЕЛ

Слика 5

ОСНОВНО ЈАВНО ОБВИНИТЕЛСТВО
РО бр.
Скопје,.........година

ДО
Одговорното лице на
„име на интернет сервис провајдер“
Адреса

Врз основа на член 6 ст.4 и 6 од Законот за меѓународна соработка во кривичната материја, го поднесува следното

БАРАЊЕ ЗА МЕЃУНАРОДНА ПРАВНА ПОМОШ

До Основното јавно обвинителство Скопје од страна на МВР, БЈБ, ЦПС, Центар за полициски служби, Сектор за компјутерски криминал и дигитална форензика доставено е барање бр......................., за добивање податоци од *„име на интернет сервис провајдер*“, во врска со пријава од ...., во која се наведува дека од профилот „......................“ регистриран на *„име на интернет сервис провајдер*“ биле упатени индиректни закани кон .... и неговото семејство.

Заради надлежно предметно постапување на ова обвинителство и прибирање на докази во кривичната постапка кои се однесуваат на стореното кривично дело, потребно е од страна на одговорно лице од *„име на интернет сервис провајдер*“ да ни бидат доставени следните податоци:

- Логови и ИП адреси од пристапувањето на профилот регистриран кај *„име на интернет сервис провајдер*“.

Податоците кои се бараат потребно е да содржат точен час, датум, како и временска зона.

Барањето на податоци се спроведува преку Министерството за правда.

ЈАВЕН ОБВИНИТЕЛ

Слика 6

BASIC PUBLIC PROSECUTION OFFICE
PO no.
Skopje,.........

TO
Responsible person at
„name of the internet service provider“
Address

On the basis of article 6 para (4) and (6) of the Law on the International Cooperation in Criminal Matters, the BPPO is issuing this

REQUEST FOR MUTUAL LEGAL ASSISTANCE

With its submission no........... the Ministry of Internal Affairs has requested this Prosecution Office to obtain information from the *"name of internet service provider"* in relation to an application made by ...., who claims to have received insults and threats against himself/herself and his/her family from the profile "......................" registered with the "*name of internet service provider*".

To be authorized for further proceeding upon this case and to collect the necessary evidence for the criminal procedure in relation to the committed crimes, the Basic Public Prosecution Office is requesting the authorized person of the *"name of the internet service provider"* provide the following data:

- Logs and IP addresses used for the access to the profile "……………" registered at the *"name of internet service provider"*

The above data should contain reference to the precise times, dates and time zones.

This Mutual Legal Assistance Request is forwarded via the electronic communications channel of the Ministry of Justice.

PUBLIC PROSECUTOR

Слика 7

4.3 Соработка со странски интернет провајдери од кои најчесто се обезбедуваат компјутерски податоци

Секој странски интернет провајдер има сопствени постапки и механизми преку кои на органите кои го спроведуваат законот им се обезбедуваат компјутерски податоци кои може да претставуваат потенцијален доказ во одреден кривичен предмет. Подолу е претставен краток преглед на странските интернет провајдери до кои домашните јавни обвинители и полициски службеници најчесто доставуваат барања за обезбедување на компјутерски податоци.

➢ *Facebook*

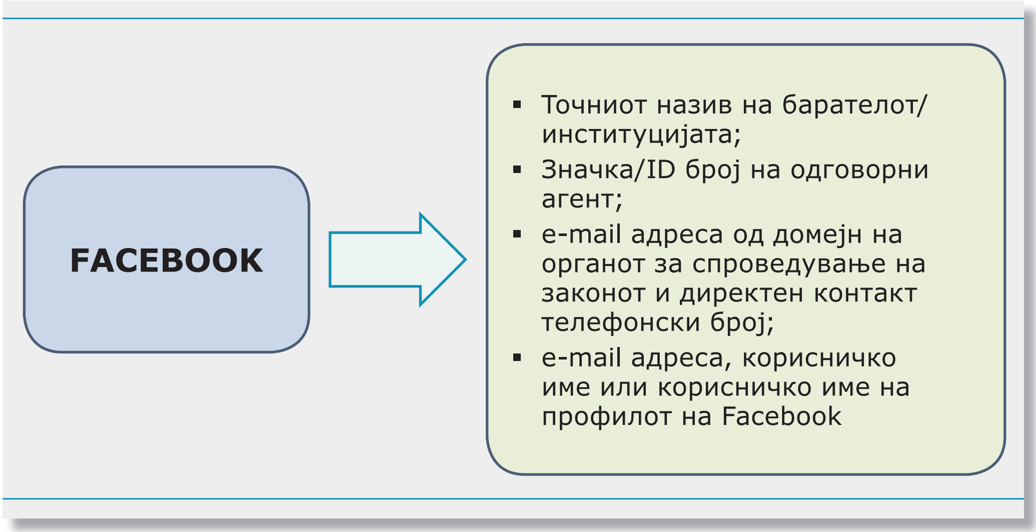
За да може Facebook да ги достави потребните податоци до органите за спроведување на законот, потребно е да се поднесе барање за меѓународна правна помош или барање од надлежна служба. За истраги кои ги водат држави со јурисдикција која не припаѓа на САД, Facebook може да одговори на барањата за обезбедување на компјутерски податоци. Информациите за постапките и механизмите за обезбедување на компјутерски податоци Facebook ги објавува на својот веб-сајт заедно со општи информации за вкупниот број на поднесени барања од секоја држава.

Во ситуации кога е потребно одредено време за да се процесуира формално правната постапка од државата барател на податоци, Facebook може да ги чува побараните компјутерски податоци. Барањето (повеќе како замолница) да се зачуваат одредени податоци до моментот на пристигнување на формалната правна документација може да се направи преку онлајн систем за поднесување на барање од страна на јавното обвинителство или полицијата, преку електронска пошта, факс или редовна пошта. Рокот за зачувување на податоците е максимум до 90 дена и доколку во тој период Facebook не ја прими формално потребната правна документација податоците нема да бидат достапни.

Во случаи кои вклучуваат непосредна повреда на дете или ризик од смрт или тешка телесна повреда на било кое лице поради што потребни е откривање на информации, без одлагање,

полициски службеник или јавен обвинител може да поднесе барање преку онлајн систем за поднесување на барање. Не ретко во практиката се случува корисникот чии податоци се побарани да не биде известен за барањето бидејќи неговото известување може да ја загрози истрагата или да доведе до ризик од друг облик. Во такви случаи Facebook треба да добие соодветна **судска одлука** која од Facebook бара да не го известува корисникот.

Барањата кои се многу општи или се нејасни, Facebook нема да ги обработува. Подолу на слика 8 е претставено што секое барање задолжително треба да содржи. Барањата се доставуваат преку системот за барања до кој имаат пристап органите за спроведување на законот на https://www.facebook.com/records

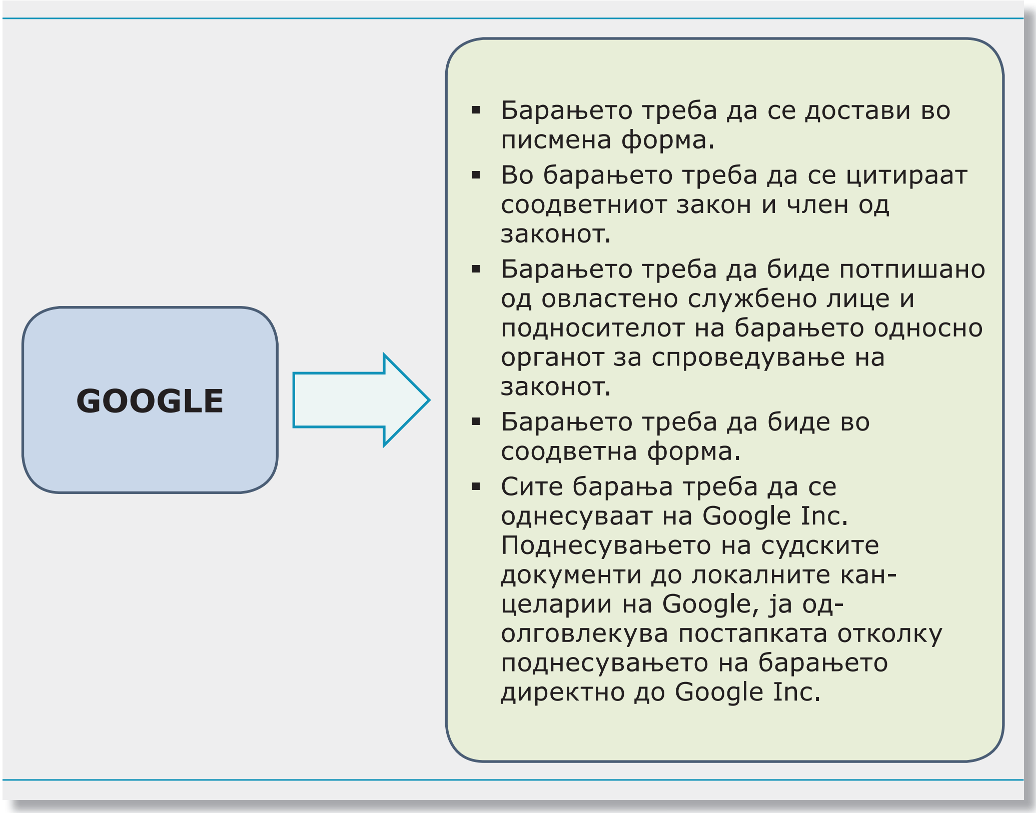


Слика 8

➤ *Google*

За обезбедување на компјутерски податоци од Google, барателот треба да достави писмено барање потпишано од овластено службено лице на подносителот на барањето иорганот за спроведување на законот, издадено врз основа на закон. За барања од надвор од САД треба да се користи механизмот за меѓусебна правна помош. Сепак, дополнително, на доброволн-

на основа, Google може да обезбеди податоци за корисниците, врз основа на соодветно барање од не-американските владини агенции. Барањата мора да бидат во согласност со меѓународните норми, законите во САД, политиките на Google и законот на земјата од каде е барањето. Сите барања за податоци за содржина треба да се доставаат во електронска форма односно преку меѓународна правна помош (MLAT), исто така можат да се добијат податоци од компанијата доколку се работат заеднички истраги меѓу САД и националните органи за спроведување на законот или доколку барањата се за итни случаи. Покрај овие процедури Google Inc може да обезбеди податоци за корисниците, на соодветно барање на соодветна агенција за спроведување на законот на доброволна основа, ако тие барања се во согласност со меѓународните норми, американските закони, политики на Google и законот на државата барател.



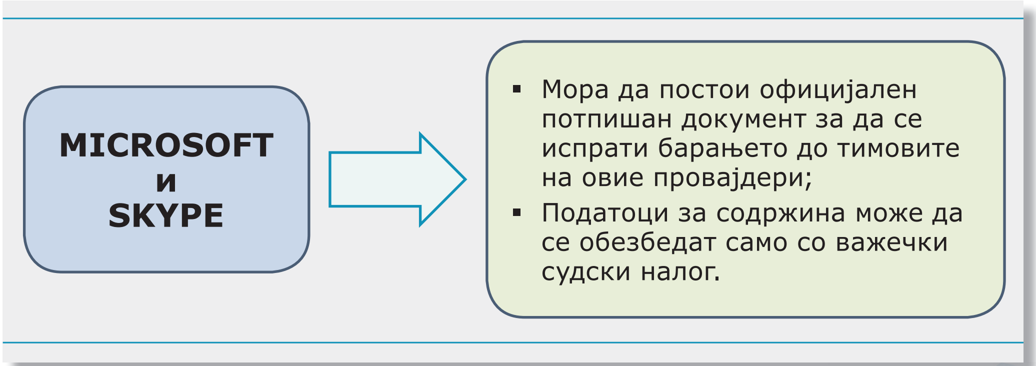
Слика 9

Слично како Facebook, и Google информациите за постапките и механизмите за обезбедување на компјутерски податоци ги објавува на својот веб-сајт заедно со општи информации за вкупниот број на поднесени барања од секоја држава. На сличен принцип како и другите странски интернет провајдери, Google не ги обработува премногу општите или нејасни барања. На нивниот веб-сајт постои водич за тоа како да се формулира барање кое ќе биде во некоја прифатливата форма. За да може да постапи по формално барање за компјутерски податоци Google бара да се исполнат критериумите посочени на слика 9.

➢ *Microsoft*

Постапката за спроведување на барањето од органите за спроведување на законите, која вклучува информации за нивните принципи, политики и практики, Microsoft исто така ја има објавено на својот веб-сајт. Принципите, политиките и практиките содржани во овој документ се однесуваат на двете компании Microsoft и Skype. Skype е независен провајдер, но во целосна сопственост на Microsoft.

Microsoft прави јасна разлика помеѓу податоци за содржина и податоци кои не се содржина. Пред податоците да бидат доставени до органите за спроведување на законите, овој провајдер треба претходно да добие важечки судски налог или еквивалентен документ. И двете компании Microsoft и Skype бараат официјален, потпишан документ издаден во согласност со локалните закони и правила за да можат истите да се доставатдо нивните тимови во САД и Ирска (Microsoft) и Луксем-



Слика 10

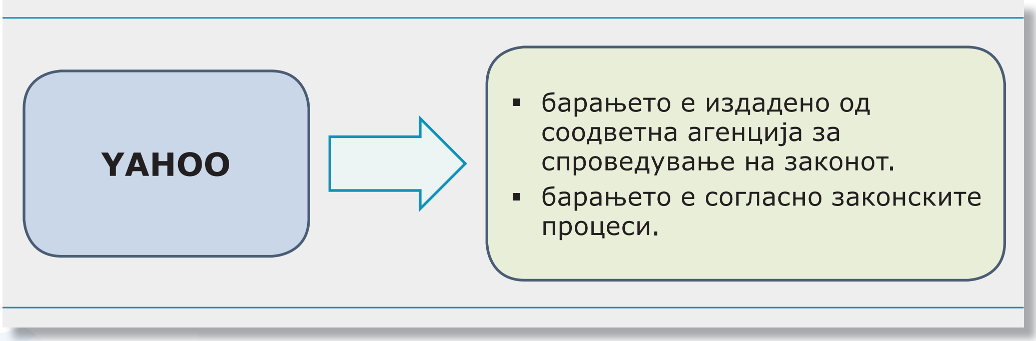
бург (Skype). Барањата за податоци кои стигаат до Microsoft од не-англиско говорно подрачје, се испраќаат до локален тим или поединец (обично адвокат или некој што работи согласно законски насоки) за усогласност со локалните закони, во кој случај барањето ќе биде преведено и испратено во тимовите на Microsoft во САД или Ирска.

Горе споменатата постапка, не ги наведува специфично условите на постапување при итни барања. Но, во документот се наведува дека Microsoft до органите за спроведување на законите може да достави ограничени информации за корисникот, односно доставува само информации за кои самиот провајдер има причина да верува дека корисникот има за цел на себе или некој друг да наштети со јавно објавување на истите информации. Барањата кои не се доставени во соодветна форма или се премногу општи, се отфрлаат и од страна на Microsoft и од Skype.

➢ *Yahoo*

Yahoo исто така соработува со органите за спроведување на законот од држави надвор од САД. По исклучок, доколку се работи за итен случај можна е директна соработка, но во сите останати ситуации барањето за обезбедување на компјутерски податоци се спроведува постапката за меѓународна правна помош.

Сите барања кои се испратени директно до Yahoo од страна на странски органи за спроведување на законот нема да бидат обработени. Ваквите барања обично се отфрлаат, освен во итни случаи кога Yahoo обезбедува одговор (на пр: киднапирање



Слика 11

или непосредни закани за бомба). Секое барање треба да биде доставено преку постапката за меѓународна правна помош или друга соодветна правна постапка. Сликата 11 прикажува што е потребно за барањето за компјутерски податоци да биде прифатено.

Yahoo не секогаш ги обезбедува бараните податоци, доколку сметаат дека обемот на податоци е голем или податоците не можат да помогнат во постапката тогаш согласно нивните политики можат да не одговорат на барањето или само делумно да достават податоци.

4.4. Видови достапни податоци и услови за нивно доставување

Секој интернет провајдер може да обезбеди различен вид на компјутерски податоци кои би претставувале потенцијален доказ во конкретна кривична постапка. Подолу е даден приказ на компјутерските податоци што секој од најчесто користените странски интернет провајдери може да ги обезбеди:

FACEBOOK Врз основа на барање од јавен обвинител или наредба од надлежен суд може да ги обезбеди овие податоци.	*на барање од јавен обвинител:* ▪ име и презиме, ▪ информации за кредитна картичка, ▪ e-mail адреса, и ▪ последни IP адреси на најави/одјави, ако бараните податоци се достапни.
	врз основа на судска наредба: ▪ други информации за сметката, не вклучувајќи ја содржината на комуникациите, ▪ full header од испратените и примените пораки.

Табела 1

GOOGLE Обезбедува податоци на органи за спроведување на законот од САД, а барањата од други земји, доколку се во согласност со меѓународните норми, законите на САД, политиките на Google и законот на земјата-барател можат да бидат одговорени на доброволна основа од страна на Google. Барањата мора да бидат во писмена форма, потпишани од овластено службено лице на подносителот на барањето.	*врз основа на наредба на обвинител:* ▪ Податоци за корисникот за регистрирање и IP адреси со кои е најавувано, со точен датум и време. ▪ Податоци за регистраторот на страната, профилот.
	врз основа на судска наредба: ▪ Податоци за интернет сообраќајот/логови; ▪ Податоци за фајлови и содржина која е објавена; ▪ IP адреси со време и датум за пристапување до содржини
	по наредба за пребарување: ▪ E-mail содржини и информации за отворени сметки на Google; ▪ Видео и друг вид материјал објавен на YouTube; ▪ Сочувани текстови и пораки на Google

Табела 2

MICROSOFT За бараните податоци мора да има судски налог или официјално потпишан друг еквивалентен документ во зависност од видот на податокот што се побарува. Microsoft обезбедува различен вид податоци за барателите кои се од САД и за оние кои се од други држави.	*За барања од САД:* ▪ Податоци за корисникот, основните податоци за претплатниците (e-mail адреса, име, адреса и IP адреса во времето на регистрација) или други податоци кои не се податоци за содржина (IP адреси на конектирање и кредитна картичка или други информации за наплата); ▪ Податоци за содржина, вклучувајќи ја содржината на пораки и документи зачувани во One Drive или други cloud сервиси.
	За барања од други држави: ▪ основни податоци за претплатниците и податоци за интернет сообраќајот (барањата треба да бидат адресирани директно до нивната канцеларија во Република Ирска).

Табела 3

YAHOO Бараните податоци може да се обезбедат само преку меѓународна првна помош. Само по исклучок доколку се работи за итна ситуација можен е директен контакт на барателот со Yahoo.	*За барања од САД:* ▪ Податоци за интернет сообраќајот, врз основа на наредба ▪ Податоци за содржина, врз основа на наредба ▪ Податоци за корисникот, врз основа на наредба	*За барања од други држави:* ▪ основни податоци за претплатниците, за испратени барања директно до Yahoo.

Табела 4

4.5 Итни барања за зачувување на податоците

Facebook - прифаќа директни барања за зачувување на податоци во врска со официјална кривична истрага за период од 90 дена додека го чека формалното барање.

Google - во пракса може да зачува податоци врз основа на барања директно добиени од органите за спроведување на законот. Потребно е официјално барање испратено преку e-mail. Google ќе ги зачува бараните податоци до пристигнувањето на официјалното барање преку постапката за меѓународна правна помош.

Microsoft - може да зачува податоци врз основа на барања директно добиени од странски органи за спроведување на законот и бара претходно по факс да биде испратено потпишано писмо. Microsoft може да ги сочува податоците за период од 180 дена и дополнително за период од 90 дена, до пристигнувањето на официјалното барање преку постапката за меѓународна правна помош.

Yahoo - може да зачува податоци врз основа на барања директно добиени од странски органи за спроведување на законот, и исто така бара претходно по факс да биде испратено потпишано писмо. Yahoo може да ги зачува податоците за 180 дена и дополнително за период од 90 дена, до пристигнувањето на официјалното барање преку постапката за меѓународна правна помош.

4.6 Постапки за испраќање на барања во итни случаи

Facebook - во итен случај, вклучувајќи непосредна повреда на дете или ризик од смрт или сериозни физички повреди на кое било лице, Facebook, без одлагање, доставува податоци до службеното лице од органот за спроведување на законот. Барањата треба да бидат поднесени преку on-line системот за прием на барања на органите за спроведување на законот https://www.facebook.com/records/x/login/ или преку електронска пошта.

Google - при итни постапки Google доброволно доставува информации до службеното лице од органот за спроведување на законот кога се верува дека тоа е неопходно за да се спречи смрт или сериозни физички повреди на некого. За итните случаи барањата мора да содржат опис на причината за итност и објаснување за тоа како информациите кои се бараат може да ја спречат штетата. Податоците кои ги обезбедуваат како одговор на барањето се ограничени на тоа што Google смета дека ќе помогне да се спречи злоупотребата или заканата.

Microsoft – може во ограничени случаи да достави информации, на пример кога е неопходно за да се спречи итна закана или опасност од смрт или сериозни физички повреди на луѓето. Ваквите барања мора да бидат во писмена форма на официјален меморандум, потпишан од страна на службениот претставник на органот за спроведување на законот. Барањето мора да содржи резиме на вонредната состојба, заедно со објаснување за тоа на кој начин информациите побарани од Microsoft ќе помогнат за спроведување на законот во решавањето на конкретниот итен случај. Пред какви било податоци да се доставаат до барателот секое барање внимателно се оценува од страна на тимот на Microsoft.

Yahoo - потребно е да се доставаат доволно информации во барањето со цел да се заклучи дека доставувањето на податоци без одлагање е потребно за да се спречи опасност од смрт или тешка телесна повреда на некое лице. Сите барања за доставување на податоци за итни случаи треба да бидат доставени до Yahoo во писмена форма, по што ќе се оценува дали барањето за итно доставувањето на податоци е релевантно. Yahoo има право да споделува само информации кои верува дека се потребни да се спречи одредена вонредна ситуација.

4.7 Зачувување на податоци

Директивата на Европската Унија 2006/24/ЕС како регулатива за зачувување на податоци има за цел да го усогласи времетраењето на периодот во кој провајдерите на електронски комуникации ги чуваат податоците од комуникацискиот сообраќај. Членот 6 од Директивата бара земјите членки на ЕУ да ги задржат податоците од сообраќајот за период не помал од 6 месеци, а не подолг од 24 месеци. Повеќето земји членки во имплементацијата на Директивата избрале да побараат од своите национални комуникациски провајдери да ги сочуваат податоците 12 месеци. Слични напори за законско уредување на минималниот период за чување за провајдерите на услуги се подготвуваат во многу земји. Зачувувањето на податоци е особено важно за да се обезбедат доказите кои би им биле неопходни на истражните органи во конкретна кривичен предмет (на пр. обезбедување на податоци за електронските комуникации на одредено физичко лице и нивната содржина).

Понекогаш и задолжителното задржување од 12 месеци во одредени случаи може да не е доволно за да се обезбеди бараните податоци од сообраќајот сè уште да бидат достапни. Причините за ова можат да бидат повеќе. Така може да помине подолго време од моментот кога делото било сторено до правната квалификација на истото и покренувањето на истрагата. Понатаму, претходната постапка може да потрае додека се идентификуваат ресурсите на интернет што биле користени од сторителот бидејќи можеби користел посредни чекори кои мора да се анализираат еден по еден. Конечно, процесуирањето на формалното барање низ дипломатските канали за да биде доставено до интернет провајдерот исто така бара дополнително време.

Од овие причини членот 16 од Европската конвенција за компјутерски криминал ЕТС 185, на земјите членки им дозволува да побараат зачувување на компјутерските податоци, како на пример содржината на сметката на електронската пошта, дури и пред да се добие законско одобрение за размена на податоци. Членот 17 за податоци од сообраќајот покрај воспоставувањето на постапка за барање на брзо зачувување на податоците дозволува и делумно обелоденување на информациите на забрзан начин. Одредена земја може да побара од друга членка податоци од сообраќајот и од содржината да се зачуваат пре-

ку мрежата за контакт која функционира 24/7 и е креирана со членот 35 од Конвенцијата.

Кога ќе се направи барање за зачувување на податоци препорачливо е органот на прогонот што го поднел барањето да побара потврда дека податоците биле сочувани и да му се даде референтен број за сочуваните податоци.

Сепак, согласно Конвенцијата, не е задолжително да се користи мрежата за контакт која функционира 24/7 за барања за зачувување. Доколку националното процесно право го дозволува тоа, директната соработка меѓу провајдерите и органите на прогонот е исто така можна, и таа потенцијално може да биде пофлуидна и со подобро разбирање на идеите и ограничувањата на страните. Директната соработка меѓу органите на прогонот и провајдерите во однос на барањата за зачувување, наместо преку мрежата за контакт 24/7 која повеќе е од дополнителен карактер, честопати е пофлексибилно решение отколку воспоставените формални контакт точки на Конвенцијата.

Слично како претходно, подолу во текстот е претставен еден пример за содржината на барање зачувување на комјутерски податоци кои би можеле да бидат потенцијален доказ во одредена кривична постапка. Од истите причини како погоре предлог образецот е даден на англиски јазик.

Data Preservation Request

First request: ❒ Yes ❒ No

Ticket number of the previous request (if available): ....

REQUESTED AUTHORITY
REFERENCE / CASE NUMBER
REQUESTING AUTHORITY

❒ Please be informed that we intend to submit a request for mutual legal assistance to obtain production of the data.

DATE
DD/MM/YYYYY
SUBJECT/TITLE
PURPOSE OF THE REQUEST
URGENCY
❒ **URGENT** Response expected by: DD/MM/YYYY
REASONS FOR URGENCY ❒ Threat to life and limb ❒ Offender in custody ❒ Crime in progress ❒ Volatility of data ❒ Imminent threat of a serious nature to public security ❒ The only evidence available ❒ Statute of limitation due to expire ❒ Other:……………………………………………………………………………
DESCRIPTION/JUSTIFICATION FOR URGENCY
CONFIDENTALITY
❒ The data submitted is only for request purpose ❒ The data submitted can be used by the requested authority ❒ The data submitted can be shared with other authorities

OFFENCES SUBJECT TO CRIMINAL INVESTIGATION OR PROCEEDINGS

(Irrespective of their consideration in the requested State)

OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND SYSTEMS / COMPUTER-RELATED OFFENCES
[click to select]
OFFENCES RELATED TO ORGANIZED CRIME AND CORRUPTION
[click to select]

OFFENCES AGAINST THE PERSON
[click to select]
OFFENCES OF FRAUD/FINANCIAL OFFENCES
[click to select]
OTHER SERIOUS OFFENCES
[click to select]
ANY OTHER OFFENCE (PLEASE SPECIFY)
HOW IS THE DATA RELATED TO THE INVESTIGATION
APPLICABLE LEGISLATION (SUBSTATIVE AND/OR PROCEDURAL) Please cite the most relevant
Title of Legislation
Relevant Sections
Right to Request Data
Codes of Practice
Relevant Court Decisions
CASE STATUS
❒ Pre-investigative phase ❒ Investigate phase ❒ Prosecution phase ❒ On trial Other details: ....

DATA TO BE PRESERVED	
❒ **Subscriber information**	Please specify: ....
Period of interest	Start date: DD/MM/YYYY End date: DD/MM/YYYY
❒ **Traffic data**	Please specify: ....
Period of interest	Start date: DD/MM/YYYY End date: DD/MM/YYYY
❒ **Content data**	Please specify: ....
Period of interest	Start date: DD/MM/YYYY End date: DD/MM/YYYY

EXPECTED ANSWERS/RESULTS
❒ Confirmation for receiving the request ❒ Confirmation for preservation of the data ❒ Information of the amount of data preserved ❒ Information of the type of data preserved ❒ Information on the preservation period ❒ Information on legal procedure used for preservation ❒ Other: …………………………………………………………………………………………..
EXPEDITED DISCLOSURE OF PRESERVED TRAFFIC DATA (UNDER ART. 30) Details/description of data

REQUESTING AUTHORITY DETAILS	
Name	
Address	
Telephone number	
Cell phone number	
E-mail address	
Fax number	
Office Hours	
Time Zone	
FOR VERIFICATION BY THE AUTHORISED PERSON, PLEASE CONTACT:	
Name:	
Job Title:	
Function:	
Signature:	

❒ Please let us know if, according to this information, you intend to build a criminal case within your country.

❒ Please let us know if you encounter issues taking into account this request.

❒ If the system is a shared system, please preserve all basic subscriber information for all virtual systems on the IP.

ANNEX: DATA SPECIFICATION FORM		
Brief description of the request:		
IPv4	**1-255**	**1-255**
URL:		
Date		
Time		
Time Zone		
Proxy		
Anonymization		
IPv6	**Subnet – 64 bit**	**Host – 64 bit**
URL:		
Date		
Time		
Time Zone		
Proxy		
Anonymization		
Other data		
E-mail address		
Social Networking ID		
Date		
Time		
Time Zone		
Proxy		
Anonymization		
Details of person or organization		
Business Name		
Legal Name		
Contact name		
Address		
Country		
Phone		
Email		
Address		

5. НАМЕСТО ЗАКЛУЧОК

Со брзиот развој на технологијата и распространета употреба во сите сфери на општественото живеење, сосема очекувана е нејзината применливост при извршувањето на кривичните дела. Техничките можности кои секојдневно се усовршуваат го подигнуваат начинот на комуникација на едно сосем поинакво ниво. Динамичниот развој на технолошките алатки неминовно бараат специфична подготвеност на органите на прогонот, особено на јавните обвинители, во процесот на откривање на сторителите на кривични дела.

Обезбедувањето на компјутерски податоци кои би можеле да претставуваат доказ во одредена кривична постапка не е секогаш едноставно. Напротив, во повеќето предмети, она што е можеби приоритет за домашните органи, за странскиот интернет провајдер од каде треба да се обезбеди податокот, тоа можеби не е така. Дополнително секој од овие провајдери има сопствени регулативи и протоколи кои се во согласност со законската рамка на земјата во која тие се регистрирани.

Обидите на глобално ниво да се прифатат заеднички минимум стандарди и принципи ја олеснуваат комуникацијата меѓу државите и нивните органи на прогон. Сепак, времето, кое можеби е и еден од најзначајните чинители во овие постапки, не е сојузник на органите кои ги откриваат и гонат сторителите на кривични дела.

Во секој случај, од исклучително значење за зголемување на ефикасноста при постапувањето во овие кривични предмети е воедначената практика на јавните обвинители при кординирање на полицијата и при поднесувањето на барањата за обезбедување на компјутерски податоци. Предлог образците кои се дадени во овој Краток водич се всушност мал допринос кон таквата сообразност при постапувањето и се надеваме дека ќе бидат од корист и за јавните обвинители и за полициските службеници.

ПРИЛОГ 1: Листа на адреси на интернет сервис провајдери

1. AMAZON.COM, INC.

Веб страна: www.amazon.com
Други сервиси: aws.amazon.com; Kindle
Адреса:
Corporation Service Company
Attn: Legal Department - Subpoena
Amazon.com Inc.
300 Deschutes Way SW, Suite 304
Tumwater, WA98501
Контакт: Преку е-маил за сите правни барања. Барање за зачувување на податоци може да се прати на subpoena@amazon.com

2. APPLE, INC.

Веб страна: www.apple.com
Други сервиси: Filemaker; iDisk; mac.com; me.com; mobileme.com
Адреса:
Attention: Apple Litigation Group
AppleInc.
1 Infinite Loop M/S: 169---2NYJ
Cupertino, CA95014---2084
Телефон: +1-408-974-8100
Fax: +1-408-974-9316
Email: subpoenas@apple.com
Контакт за итни барања: +1-408-974-2095, Global Security Operations Center (GSOC)
Постапка за соработка со органите за спроведување на закони: http://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf

3. FACEBOOK, INC.

Веб страна: www.Facebook.com
Адреса:
Facebook, Inc.
Attn: Facebook Security, Law Enforcement Response Team
1601 Willow Road
Menlo Park CA 94025
Телефон: +1-650-543-4938
Fax: +1-650-472-8007

Email: records@facebook.com
Контакт за итни барања: www.facebook.com/records (барањето да биде насловено со ”EMERGENCYREQUEST”)
Извештај за транспарентност: https://govtrequests.facebook.com/country/Macedonia/2016-H2/

4. GOOGLE, INC.

Веб страна: www.Google.com
Други сервиси: Blogger/Blogspot; BlogSpot; FriendConnect; Gmail; GoogleLatitude; GoogleVoice; Orkut; Picasa; YouTube
Адреса:
Custodian of Records
Google
1600 Amphiteatre Parkway
Mountain View, CA94043
Телефон: +1-650-253-3425
Email: LIS-GLOBAL@google.com
Контакт за итни барања: +1-650-253-3425 (Call Center)
Постапка за соработка со органите за спроведување на закони: https://www.google.com/transparencyreport/userdatarequests/legalprocess/

5. MICROSOFTCORPORATION, INC.

Веб страна: www.msn.com
Други сервиси: Bing; domains.live.com; groups.msn.com; Hotmail; live.com; live.net; live@edu; MicrosoftOfficeLive; MicrosoftOnlineServices; MSN; MSN, Groups; MSNHotmail; MSNSpaces; MSNTV; msn.com; officelive.com; outlook.com; Skydrive; spaces.live.com; WebTV; WindowsLiveHotmail; WindowsLiveID(Passport); WindowsLiveMessenger; WindowsLiveServices; WindowsLiveSpaces; Xbox; Xbox360; XboxLive.
Адреса:
Attn: Online Services Custodian of Records
Microsoft Corporation
One Microsoft Way
Redmond, WA98052---6399
Телефон: +1-425-722-1299
Fax: +1-425-708-0096
Контакт за итни барања: Call +1-425-722-1299 или email LEAlert@microsoft.com.
Извештај за транспарентност:
https://www.microsoft.com/en-us/about/corporate-responsibility/lerr

6. TWITTER, INC.

Веб страна: www.twitter.com
Адреса:
Twitter, Inc.
c/o Trust & Safety – Legal Policy
1355 Market Street, Suite 900
San Francisco, CA 94103
Fax: +1-415-222-9958
Email: lawenforcement@twitter.com
Контакт за итни барања: online форма на барање да се пополни на https://support.twitter.com/forms/lawenforcement.

7. YAHOO, INC.

Веб страна: www.Yahoo.com
Други сервиси: altavista.com; Flickr.com; rocketmail.com; Yahoo!Axis; Yahoo!Domains; Yahoo!Mail; Yahoo!Messenger; yahoo.br; yahoo.com; ymail.com
Адреса:
Yahoo!, Inc.
Attn: Custodian of Records
701 First Avenue
Sunnyvale, CA 94089
Телефон: +1-408-349-3687
Fax: +1-408-349-7941
Email: lawenforcement-request-delivery@yahoo-inc.com
Контакт за итни барања:
+1-408-349-3687 (од 8.00 до 16.00)
+1-408-349-5400 (после 16.00)
Извештај за транспарентност:
https://transparency.yahoo.com/government-data-requests