



**T-CY**  
**CYBERCRIME CONVENTION COMMITTEE**  
**COMITÉ DE LA CONVENTION CYBERCRIMINALITÉ**

T-CY(2014)17  
(Provisoire)

Strasbourg, France  
3 décembre 2014  
**(Projet de rapport)**

## **Règles concernant l'obtention de données relatives aux abonnés**

**Rapport adopté par le T-CY lors de sa 12<sup>ème</sup> Réunion Plénière (2-3 décembre 2014)**

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)



**Contact**

Alexander Seger  
Secrétaire exécutif  
Comité de la Convention sur la cybercriminalité (T-CY)  
Direction Générale Droits de l'homme et Etat de droit  
Conseil de l'Europe, Strasbourg, France

Tél. +33-3-9021-4506  
Fax +33-3-9021-5650  
Email: [alexander.seger@coe.int](mailto:alexander.seger@coe.int)

# Table des matières

<b>1</b>	<b>Contexte et finalité du rapport .....</b>	<b>4</b>
<b>2</b>	<b>Synthèse de l'expérience des Parties .....</b>	<b>5</b>
2.1	Définition du terme « adresse IP » aux fins du droit pénal .....	5
2.2	Adresse IP = donnée à caractère personnel ?.....	6
2.3	Catégories de données considérées comme des informations relatives aux abonnés.....	8
2.4	Conditions requises pour l'obtention de données relatives aux abonnés.....	17
2.5	Conditions requises pour l'obtention de données relatives à un abonné pour une adresse IP particulière dans le cadre d'une enquête pénale spécifique .....	22
2.6	Catégories de données considérées comme des données relatives au trafic .....	23
2.7	Conditions requises pour l'obtention de données relatives au trafic auprès d'un fournisseur de services dans le cadre d'une enquête pénale.....	28
<b>3</b>	<b>Conclusion.....</b>	<b>31</b>
<b>4</b>	<b>Appendix: Compilation of replies.....</b>	<b>33</b>
4.1	Australia .....	33
4.2	Austria.....	37
4.3	Azerbaijan.....	40
4.4	Bosnia and Herzegovina .....	41
4.5	Bulgaria .....	45
4.6	Croatia .....	51
4.7	Czech Republic.....	54
4.8	Denmark.....	58
4.9	Estonia .....	60
4.10	Finland .....	63
4.11	France .....	67
4.12	Germany.....	69
4.13	Japan .....	75
4.14	Latvia .....	78
4.15	Lithuania.....	80
4.16	Mauritius.....	84
4.17	Moldova .....	88
4.18	Montenegro .....	92
4.19	Norway.....	94
4.20	Portugal .....	98
4.21	Romania .....	101
4.22	Serbia.....	104
4.23	Slovakia.....	107
4.24	Slovenia.....	109
4.25	Spain.....	111
4.26	"The former Yugoslav Republic of Macedonia" .....	116
4.27	Ukraine.....	118
4.28	USA.....	121
<b>5</b>	<b>Appendix: Additional information provided .....</b>	<b>123</b>
5.1	Canada .....	123
5.2	Finland .....	123
5.3	Norway .....	123
5.4	USA.....	123
<b>6</b>	<b>Annexe: extraits de la Convention de Budapest.....</b>	<b>125</b>

# 1 Contexte et finalité du rapport

L'objectif du présent rapport est de favoriser le partage d'expériences entre les Parties à la Convention de Budapest sur la cybercriminalité concernant l'obtention de données relatives aux abonnés aux fins de la justice pénale.

Le Comité de la Convention sur la cybercriminalité (T-CY) considère qu'il s'agit là d'une question importante. L'obtention d'informations auprès de fournisseurs d'accès internet pour identifier l'utilisateur (abonné) d'une adresse spécifique de protocole internet (IP) à un moment précis ou, vice-versa, pour identifier les adresses IP utilisées par une personne déjà connue<sup>1</sup>, est essentielle dans le cadre d'enquêtes et de procédures pénales en matière de cybercriminalité et de preuve électronique. Les données relatives aux abonnés sont également les données les plus souvent recherchées dans le contexte de la coopération internationale.

Les adresses IP peuvent relever de deux catégories de données :

- Les « données relatives au trafic » telles qu'elles sont définies à l'article 1.d de la Convention de Budapest :
  - d « données relatives au trafic » désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ;*
- Les « données relatives aux abonnés » telles qu'elles sont définies à l'article 18.3 de la Convention de Budapest :
  - 3 Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :*
    - a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;*
    - b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;*
    - c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.*

Dans la mesure où la Convention de Budapest fait la différence entre « données relatives au trafic » et « données relatives aux abonnés », différentes règles peuvent s'appliquer pour l'obtention de chacune de ces catégories de données. Les adresses IP peuvent être considérées comme des données relatives aux abonnés – par opposition à données relatives au trafic – si l'objectif est d'obtenir l'identification d'un abonné utilisant une adresse IP.

Le T-CY, lors de ses 10<sup>e</sup> (décembre 2013) et 11<sup>e</sup> réunions plénières (juin 2014) a examiné un projet de Note d'orientation sur « l'obtention, dans le cadre d'une enquête pénale, de données relatives aux abonnés utilisant une adresse IP pour une communication spécifique » (document T-CY(2013)26) ainsi que les informations transmises par les Parties en réponse à un questionnaire.

Toutefois, le T-CY a considéré que « l'adoption d'une note d'orientation sur les informations relatives aux abonnés reflétant l'interprétation commune des Parties serait prématurée étant donné la diversité des règles, conditions et procédures dans les Etats parties » et demandé au Secrétariat « de

---

<sup>1</sup> Voir paragraphe 178 du rapport explicatif de la Convention de Budapest sur la cybercriminalité.

transformer le résumé des réponses au questionnaire en un rapport à part entière ». Il a par ailleurs encouragé « les Parties à tenir compte des observations de ce rapport lors de la refonte de leur législation interne »<sup>2</sup>.

Le présent rapport a été adopté lors de la 12<sup>ème</sup> Réunion plénière du T-CY les 2 et 3 décembre 2014.

## **2 Synthèse de l'expérience des Parties<sup>3</sup>**

### **2.1 Définition du terme « adresse IP »<sup>4</sup> aux fins du droit pénal**

**Question 1 : Existe-t-il, dans votre droit interne, une définition du terme « adresse IP » à des fins pénales (lois ou dispositions pénales, réglementaires ou techniques, etc.) ? Si oui, veuillez fournir les textes légaux ou réglementaires correspondants.**

Les réponses transmises révèlent que, dans la plupart des Etats, il n'existe pas de définition spécifique du terme « adresse IP » aux fins du droit pénal.

Les réponses peuvent être classées en quatre catégories :

1. Dans quelques Etats, les adresses IP, ou un équivalent, sont évoquées dans le droit pénal ou dans d'autres réglementations comme pouvant être utilisées aux fins du droit pénal. Par exemple :
  - La Finlande parle de « données d'identification » qu'elle définit à l'article 2, paragraphe 8 de la loi sur la protection de la vie privée dans les communications électroniques (516/2004) ;
  - En Norvège, une adresse IP renvoie à une « adresse de communication électronique », loi relative aux communications électroniques de juin 2014 2003, article 2-9;
  - La Serbie utilise les termes « adresse » et « numéros », loi relative aux communications électroniques ;
  - Le terme « adresse de télécommunication » a été défini par la législation pénale en Bosnie-Herzégovine<sup>5</sup>.
2. Plusieurs Etats utilisent le terme « adresse IP » ou un équivalent dans leurs différentes réglementations sans préciser si ces définitions peuvent être utilisées aux fins du droit pénal :

---

<sup>2</sup> [http://www.coe.int/t/dqhl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY\(2014\)11\\_Plen11AbrRep\\_V4.pdf](http://www.coe.int/t/dqhl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)11_Plen11AbrRep_V4.pdf)

<sup>3</sup> Sur la base des réponses au questionnaire reçues en mars et en avril 2014.

<sup>4</sup> Le terme « adresse IP » (IP pour Internet Protocol) désigne la série de chiffres séparés par des points utilisée pour caractériser et identifier un ordinateur sur internet. L'adresse IP est attribuée automatiquement par les fournisseurs d'accès internet chaque fois qu'un ordinateur se connecte à internet.

Aux fins de l'identification d'un abonné, il convient de faire la distinction entre adresse IP « statique » et adresse IP « dynamique » : une adresse IP statique est attribuée à un client spécifique alors qu'une adresse IP dynamique est attribuée temporairement quand un ordinateur se connecte à internet. Dans ce dernier cas, un horodatage (« time stamp ») est nécessaire pour identifier l'abonné.

<sup>5</sup> Code de procédure pénale (CPC) de la Bosnie-Herzégovine, CPC de la Fédération de la Bosnie-Herzégovine, CPC de la Republika Srpska, CPC de Brcko District de la Bosnie-Herzégovine.

- Autriche : définition d'adresse IP § 92 (3) Z 16 Telekommunikationsgesetz (TKG) 2003
  - Bulgarie : définition d'adresse IP dans la loi relative aux jeux d'argent de 2012;
  - Croatie : définition du terme « adresse de télécommunication électronique » dans loi relative aux communications électroniques, article 2, paragraphe 1, alinéa 1;
  - République tchèque : définition d'une « adresse IP » aux fins de la réglementation n° 357/2012
  - Japon : définition d'adresse IP à l'article 24.5.14 des « Dispositions pour la mise en œuvre de la loi sur les télécommunications »
  - La Lituanie parle de « numéro d'équipement terminal », au paragraphe 4 de la Description des conditions générales pour l'exercice d'activités de communications électroniques
  - Le Monténégro propose une définition du terme « adresse » dans sa loi sur les communications électroniques
  - La Roumanie définit la notion de « point terminal » dans sa loi n° 301/2003 sur le service universel et les droits des usagers concernant les réseaux et les services de communications électroniques
  - Slovaquie : note méthodique du ministère des Finances sur la base de la loi n° 275/2006 Rec. relative aux systèmes d'information de l'administration publique et pour modifier ou compléter certaines lois telles que modifiées par la loi n° 678/2008 Rec.
  - L'Ukraine donne une définition de ce qu'on entend par numéro et adresse d'un abonné sur l'internet, loi sur les télécommunications (article 1).
3. La législation interne des Etats suivants ne contient pas de définition du terme « adresse IP » ou équivalent : Australie, Azerbaïdjan, Estonie, France, Allemagne, Lettonie, Moldova, Portugal, Slovénie et Espagne ;
4. Les Etats suivants ont indiqué qu'ils n'avaient pas de définition d'adresse IP aux fins du droit pénal : Danemark, Japon, Maurice et Etats-Unis.

## **2.2 Adresse IP = donnée à caractère personnel ?**

**Question 2 : Une adresse IP est-elle considérée comme étant une donnée à caractère personnel ? Si oui, veuillez fournir le texte correspondant.**

Les réponses à cette question montrent que les avis divergent quant au fait de considérer ou non les adresses IP comme des données à caractère personnel. Bien qu'il n'y ait pas de consensus international sur la question, le point de vue qui prévaut au niveau européen et international semble être que les adresses IP sont considérées comme des données à caractère personnel dès lors qu'elles permettent d'identifier un individu. Que cette identification soit possible, ou le soit sans impliquer d'effort démesuré, dépend du contexte<sup>6</sup>.

---

<sup>6</sup> Avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf)

Protection of personal data on-line: the issue of IP addresses, by Peter J. Hustinx, Article published in Revue Légicom no. 42, first issue 2009.

[https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-04-15\\_adresses\\_IP\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-04-15_adresses_IP_EN.pdf)

D'après les réponses reçues, les adresses IP sont considérées comme des données à caractère personnel dans les pays suivants :

- Autriche : § 92 (3) Z 16 letzter Satz TKG 2003;
- Croatie : loi sur la protection des données à caractère personnel (article 2, paragraphe 1, alinéa 1);
- République tchèque : article 4 point a) de la loi n° 101/2000 Rec. sur la protection des données à caractère personnel ;
- Estonie : loi sur la protection des données à caractère personnel, article 4 « données à caractère personnel » ;
- Allemagne : uniquement pour les adresses IP statiques, article 3 de la loi fédérale sur la protection des données à caractère personnel, par extension aux adresses IP dynamiques ;
- Japon : loi sur la protection des informations à caractère personnel (toutefois la définition de « données à caractère personnel » n'est pas la même que celle figurant dans la Convention 108);
- Slovaquie : une adresse IP est considérée comme une donnée à caractère personnel (article 5 du décret du ministère de la Justice de la République de Slovaquie n° 482/2011 Rec.);
- Espagne : dans son rapport 327/2003, l'agence pour la protection des données (AEPD) considère que « les adresses IP, qu'elles soient fixes ou dynamiques, indépendamment du type d'accès, doivent être considérées comme des données à caractère personnel » ;
- Etats-Unis<sup>7</sup>.

D'autres Etats indiquent que, à la lumière de la définition de « données à caractère personnel », les adresses IP peuvent être considérées comme des données à caractère personnel si elles se rapportent à une personne identifiée ou identifiable :

- Australie ;
- Bosnie-Herzégovine, loi sur la protection des données à caractère personnel de la Bosnie-Herzégovine (Journal officiel de Bosnie-Herzégovine, n° 49/06, 76/11 et 89 /11, article 3);
- Bulgarie : loi sur la protection des données à caractère personnel ;
- Danemark : loi sur le traitement des données à caractère personnel ;
- Finlande : loi sur la protection des données à caractère personnel (523/1999), article 3 alinéa 1 ;
- Lituanie : loi sur la protection juridique des données à caractère personnel (article 2§1)
- Maurice : article 2 de la loi sur la protection des données ;
- Moldova: loi n° 133 du 08.07.2011 sur la protection des données à caractère personnel, article 3 ;
- Norvège : loi sur la protection des données à caractère personnel ;
- Roumanie : loi n° 677/2001 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel (Directive 95/46/CE relative à la protection des données).

---

Voir également Considérant 24 de la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)

[http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf)

Avis 01/2012 du groupe de travail « article 29 » sur les propositions de réforme de la protection des données, adopté le 23 mars 2012 [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf)

Affaire 70/10 Scarlet c. SABAM, Cour de Justice de l'Union européenne, 24 novembre 2011

<http://curia.europa.eu/juris/document/document.jsf?docid=115202&doclang=en>

<sup>7</sup> NB: l'utilisation de « données à caractère personnel » au sens du droit pénal américain n'est pas nécessairement comparable à celle qu'en fait le droit européen sur la protection des données.

D'autres pays affirment que leur législation interne reste floue quant au statut de l'adresse IP en tant que donnée à caractère personnel :

- France, Serbie, Portugal et Lettonie.

Enfin, seuls quelques Etats ont indiqué que leur législation ne considèrerait pas les adresses IP comme des données à caractère personnel :

- Monténégro, Slovénie et Ukraine.

On peut dès lors supposer que dans la plupart des Etats parties, dans le cadre d'une enquête pénale visant à identifier l'utilisateur d'une adresse IP ou les adresses IP utilisées par une personne spécifique, il convient de considérer les adresses IP comme des données à caractère personnel.

### **2.3 Catégories de données considérées comme des informations relatives aux abonnés**

**Question 3 : Quelles sont, en vertu de votre droit interne, les catégories de données considérées comme des informations relatives aux abonnés ? Veuillez fournir le texte correspondant.**

Les données relatives aux abonnés sont la catégorie de données la plus souvent recherchée dans le cadre des enquêtes menées sur le territoire national mais aussi au niveau international.

Le paragraphe 178 du rapport explicatif de la Convention de Budapest précise que, dans le cadre d'une enquête pénale, les informations relatives aux abonnés peuvent être nécessaires « dans deux situations spécifiques » :

- « Premièrement, elles sont nécessaires pour déterminer les services et mesures techniques connexes qui ont été utilisés ou sont utilisés par un abonné, tels que le type de service téléphonique utilisé (par exemple téléphonie mobile), le type de services connexes utilisé (renvoi automatique d'appel, messagerie téléphonique, etc.), le numéro de téléphone ou toute autre adresse technique (comme une adresse électronique). »
- « Deuxièmement, lorsqu'une adresse technique est connue, les informations relatives aux abonnés sont requises pour aider à établir l'identité de l'intéressé. »

Le paragraphe 178 poursuit :

« D'autres informations relatives aux abonnés, telles que les informations commerciales figurant dans les dossiers de facturation et de paiement de l'abonné, peuvent également être utiles aux enquêtes pénales surtout lorsque l'infraction faisant l'objet de l'enquête concerne un cas de fraude informatique ou un autre délit économique. »

Le paragraphe 180 du rapport explicatif précise le spectre de données devant être considérées comme des informations relatives aux abonnés :

« Les informations relatives aux abonnés ne sont pas limitées aux informations se rapportant directement à l'utilisation du service de communication. Elles désignent également toutes les informations, autres que des données relatives au trafic ou au contenu, qui permettent d'établir l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'utilisateur, et tout autre numéro d'accès et les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou arrangement de service entre l'abonné et le fournisseur de services. »



L'article 1 d. de la Convention de Budapest définit les « données relatives au trafic » comme désignant :

« toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ».

Le paragraphe 209 du rapport explicatif explicite l'expression « données relatives au contenu » :

« Les "données relatives au contenu" ne sont pas définies dans la Convention, mais désignent le contenu informatif de la communication, c'est-à-dire le sens de la communication ou le message ou l'information transmis par la communication (autre que les données relatives au trafic). »

Au regard des réponses au questionnaire, trois situations se dégagent au sein des Etats parties concernant le concept ou la définition de « donnée relatives aux abonnés » :

- 17 Etats définissent clairement l'expression « données relatives aux abonnés » ;
- Dans 8 Etats, il est possible de déduire la signification de « données relatives aux abonnés » à partir de différents textes ;
- Seuls 3 Etats indiquent qu'ils n'ont pas de définition (ou n'ont pas répondu à la question).

### 2.3.1 Etats proposant une définition claire des « données relatives aux abonnés » et précisant les données considérées comme telles

Etat	Texte de référence	Données considérées comme « données relatives aux abonnés »
Autriche	§ 92 (3) Z 3 TKG 2003	Nom, diplôme universitaire, lieu de résidence, numéro de l'utilisateur ou tout autre numéro associé, informations sur le type et le contenu du contrat, solvabilité.
Bosnie-Herzégovine	Décision du Conseil des Ministres n° 258/06	Nom et adresse de la personne morale, physique ou de toute autre personne au nom de laquelle est enregistrée l'adresse de télécommunication.
Bulgarie	Paragraphe 2, article 248 de la loi sur les communications électroniques	Données relatives au trafic, données nécessaires à la facturation et attestant de leur fiabilité y compris les coordonnées de l'abonné et le type de services de communications électroniques ainsi que les données de localisation.
Croatie	Ordonnance sur les modalités et les conditions de la fourniture de réseaux et de services de communications électroniques (article 8)  Article 263 du Code de procédure pénale	Nom et siège social s'il s'agit de personnes morales, ou nom et adresse des utilisateurs s'il s'agit de personnes physiques, (7.) adresse du point de connexion qui permettra à l'abonné d'avoir accès au réseau public de communications, (8.) adresse pour les notifications et adresse de facturation des services de communications électroniques, (9.) adresse de courrier électronique à laquelle l'abonné souhaite recevoir une notification s'il a souscrit un abonnement d'accès à internet.  – (1) les dispositions de l'article 261 de cette loi s'appliquent également aux données sauvegardées sur l'ordinateur et aux appareils reliés à celui-ci, ainsi qu'aux appareils utilisés pour la collecte et le transfert de données, les supports de données et les informations relatives à l'abonné qui sont en possession du fournisseur de services
France	Chapitre II de l'article 6 de la loi 2204/575 du 21 juin 2004, Loi pour la confiance dans l'économie numérique et décret 2011-219 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu en ligne	– Nom, prénom, raison sociale, – adresses postales associées, – pseudonymes utilisés, – adresses de courrier électronique ou de comptes associés, – numéros de téléphone, – mot de passe ainsi que les données permettant de le vérifier ou de le modifier, – type de paiement utilisé, – référence du paiement, – montant, date et heure de la transaction.

Etat	Texte de référence	Données considérées comme « données relatives aux abonnés »
		<ul style="list-style-type: none"> <li>- identifiants de connexion à l'origine de la communication</li> <li>- type de protocoles utilisés pour la connexion au serveur, et pour le transfert des contenus</li> <li>- nature de l'opération, des dates et heures, ainsi que de l'identifiant fourni par l'auteur de l'opération lorsque celui ci l'a fourni.</li> </ul>
Allemagne	<p>Article 3, par. 3 de la loi sur les télécommunications (<i>Telekommunikationsgesetz, TKG</i>)</p> <p>Article 111 de la loi sur les télécommunications</p>	<p>« Les données relatives au client » désignent les données relatives à un abonné collectées dans le but d'établir un contrat relatif à des services de télécommunications, d'en concevoir le contenu, de le modifier ou d'y mettre fin ;</p> <p>Les fournisseurs d'accès peuvent conserver certaines données relatives au client dans le cadre de la relation contractuelle mais doivent également conserver les données suivantes pour répondre aux éventuelles demandes d'information de la part des autorités responsables de la sécurité :</p> <ul style="list-style-type: none"> <li>- le numéro de téléphone et autres identifiants,</li> <li>- les nom et adresse du titulaire du numéro d'appel,</li> <li>- la date de naissance s'il s'agit de personnes physiques,</li> <li>- l'adresse du raccordement dans le cas de raccordements de réseau fixe,</li> <li>- dans le cas où un équipement terminal mobile est mis à disposition dans le cadre d'une connexion de téléphonie mobile, le numéro d'appel de l'équipement concerné, ainsi que</li> <li>- la date effective du contrat.</li> </ul>
Maurice	Partie 1, article 2, clause « informations relatives aux abonnés » de la loi de 2003 sur l'utilisation abusive de l'informatique et la cybercriminalité	<ul style="list-style-type: none"> <li>- le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service</li> <li>- l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ; ou</li> <li>- toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.</li> </ul>

Etat	Texte de référence	Données considérées comme « données relatives aux abonnés »
Moldova	Article 2 de la loi n° 20 en date du 03.02.2009 relative à la prévention et à la lutte contre la cybercriminalité	Données relatives aux utilisateurs : toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir : le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service, l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services, toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services ;
Norvège	Loi sur les communications électroniques du 14 juin 2003, articles 2-9	Numéros de téléphone attribué dans le cadre d'un contrat ou toute autre information relative à l'abonnement, ainsi que les adresses de communications électroniques.
Portugal	L'article 14, point 4 de la loi relative à la cybercriminalité (loi n° 109/2009, du 15 septembre 2009), comporte une liste des types de données devant être considérées comme des données relatives aux abonnés	Un abonné désigne « toute personne physique ou morale partie à un contrat avec un fournisseur de communications électroniques accessibles au public, pour la fourniture de tels services ». Il est donc logique d'en déduire que les données relatives aux abonnés sont les données nécessaires aux fins de l'identification de cette partie au contrat avec un service de communications électroniques.  4 - Les dispositions de cet article s'appliqueront aux fournisseurs de services, qui pourront être tenus de communiquer les données en leur possession se rapportant à leurs clients ou abonnés, autres que des données relatives au trafic ou au contenu, en vue d'établir : - a) le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ; - b) l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services, ou - c) toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.
Roumanie	Loi n° 161/2003 transposant la Convention de Budapest relative à la cybercriminalité	Données relatives aux utilisateurs : toute donnée pouvant permettre l'identification d'un utilisateur, y compris le type de communication et le service utilisé, une adresse postale, une adresse géographique, les numéros de téléphone et autres numéros d'accès et le mode de paiement.

Etat	Texte de référence	Données considérées comme « données relatives aux abonnés »
Slovaquie	Article 56, paragraphe 3 de la loi n° 351/2011 Coll. sur les communications électroniques, telle que modifiée	<ul style="list-style-type: none"> <li>- a) nom, titre, adresse du lieu de résidence, date de naissance, numéro de carte d'identité ou de tout autre document d'identité s'il s'agit d'une personne physique, nationalité</li> <li>- b) raison sociale, siège et numéro d'identification s'il s'agit d'une personne physique/d'un entrepreneur</li> <li>- c) raison sociale, siège et numéro d'identification s'il s'agit d'une personne morale.</li> </ul>
Slovénie	Loi sur les communications électroniques (article 110):	<ul style="list-style-type: none"> <li>- nom ou raison sociale du client;</li> <li>- adresse de l'abonné ;</li> <li>- numéro de l'abonné ou tout autre élément de numérotation utilisé pour établir la connexion avec le client;</li> <li>- nom universitaire, scientifique ou professionnel du client ou son adresse de courrier électronique (disponibles à la demande de l'abonné);</li> <li>- numéro d'identification fiscale s'il s'agit d'une personne physique et numéro d'identification fiscale et d'immatriculation s'il s'agit d'une entreprise.</li> </ul>
Espagne	Circulaire 1/2013 de la Commission espagnole du marché des télécommunications sur la procédure de collecte et de diffusion des données relatives aux abonnés	<ul style="list-style-type: none"> <li>- Identification du titulaire</li> <li>- Personne physique : nom et prénom, numéro de carte d'identité, numéro d'identification fiscale, numéro de passeport ou numéro d'identification pour les étrangers</li> <li>- Personne morale : raison sociale, numéro d'identification fiscale, dénomination commerciale</li> <li>- Identification de l'utilisateur</li> <li>- Mêmes données pour les personnes physiques et morales</li> <li>- Adresse complète (identification postale de l'abonné)</li> <li>- Numéro de l'abonné (numéros individuels et/ou plages de numéros)</li> <li>- Liste des numéros associés à l'adresse postale</li> <li>- Consentement à la publication des données ou à leur utilisation à des fins commerciales ou publicitaires</li> <li>- Type de terminal, le cas échéant</li> <li>- Mode de paiement</li> </ul>
« L'ex-République yougoslave de Macédoine »	Loi sur les communications électroniques (article 4, paragraphe 8):	Le code d'identification de l'utilisateur désigne le code d'identification unique attribué à l'abonné ou à l'utilisateur inscrit donnant accès au service internet de communication ou aux services en ligne.

Etat	Texte de référence	Données considérées comme « données relatives aux abonnés »
Ukraine		Les informations en possession des opérateurs et des entreprises de télécommunications, la relation, les personnes fournissant les services de télécommunications, y compris les personnes bénéficiaires des services, leur durée, leur contenu, les moyens de transmission, etc.
Etats-Unis	18 U.S.C. § 2703(c)(2).	Informations de base relatives à un abonné dont le gouvernement peut exiger la communication au moyen d'une ordonnance de production des pièces : (A) nom ; (B) adresse ; (C) historique des connexions téléphoniques locales et longue distance, ou historique des sessions et de leur durée ; (D) durée du service (y compris la date de début du service) et types de services utilisés (E) numéro de téléphone ou d'appareil ou autre numéro d'abonné ou identité, y compris les adresses réseau attribuées à titre temporaire ; et (F) moyens et sources de paiement pour le service en question (y compris les numéros de carte ou de compte bancaires) d'un abonné.

**2.3.2 Etats ne proposant de définition des « données relatives aux abonnés » mais dans lesquels il est possible de déterminer les catégories de données considérées comme telles**

<b>Etat</b>	<b>Texte de référence</b>	<b>Présupposés</b>
Australie	Loi sur les télécommunications (interception et accès) de 1979 (loi TIA).	Les données de « non-contenu » sont traitées de la même manière et sont considérées comme des données de télécommunications : aucune différence entre les données relatives aux abonnés et les données relatives au trafic
République tchèque		Les informations relatives aux abonnés désignent les données à caractère personnel (autrement dit toute information relative à une personne spécifiée ou spécifique)
Estonie	Article 2 15) of the Loi sur les communications électroniques.	Un abonné désigne une personne qui utilise des services de communications électroniques accessibles au public en exécution d'un contrat avec un opérateur de communications pour l'utilisation des services de communications électroniques accessibles au public.
Finlande	article 36 alinéa 2 de « l'ancienne » loi sur la police (493/1995).	Les services de police sont habilités à solliciter auprès d'un opérateur de télécommunications, d'une société ou d'une association ayant souscrit un abonnement à des services de télécommunications, les informations concernant un abonnement qui ne figure pas dans un annuaire public ou les données indiquant l'accès d'un abonné aux télécommunications, une adresse électronique ou toute autre adresse de télécommunications, ou l'équipement terminal de télécommunications si, dans certains cas particuliers, ces informations sont nécessaires à l'exercice d'une mission de police. De la même manière, les services de police sont habilités à obtenir les renseignements relatifs à une adresse postale auprès des services de poste.
Japon	aucune définition.	Les informations telles que le nom d'un abonné, son adresse postale, ses coordonnées, sa date de contrat et l'adresse IP statique unique qui lui a été attribuée peuvent être considérées comme des « informations relatives aux abonnés » ;
Lituanie	Article 3 paragraphe 1 de la Loi sur les communications électroniques.	« Un abonné désigne <u>toute personne partie à un contrat</u> avec un fournisseur de communications électroniques accessibles au public, pour la fourniture de tels services ».  Présupposé : « les données relatives aux abonnés » englobent toutes les informations disponibles sur la base d'un contrat de fourniture de services de communications électroniques.

Etat	Texte de référence	Présupposés
Monténégro	Loi sur les communications électroniques.	« Un abonné désigne toute personne physique ou morale partie à un contrat avec un fournisseur de communications électroniques accessibles au public, pour la fourniture de tels services »
Serbie		Les données relatives aux abonnés sont définies par le contrat de service établi entre le fournisseur de services et l'abonné.



### **2.3.3 Etats n'ayant pas de définition de « données relatives aux abonnés »**

Seuls trois Etats parties semblent ne pas avoir de définition de « données relatives aux abonnés », à savoir, l'Azerbaïdjan, le Danemark et la Lettonie.

Il apparaît que la définition de « données relatives aux abonnés » de la majorité des Parties englobe des informations telles que l'identité de l'abonné, son adresse postale ou géographique, son numéro de téléphone et tout autre numéro d'accès ainsi que les informations relatives à la facturation et au paiement, disponibles sur la base d'un contrat ou d'un arrangement de services.

La plupart des Parties semblent considérer l'adresse IP comme étant une donnée relative à l'abonné. La question est de savoir si, et dans quelles circonstances, leur législation interne établit une distinction claire entre « données relatives aux abonnés » et « données relatives au trafic ».

## **2.4 Conditions requises pour l'obtention de données relatives aux abonnés**

### **Question 4 : Quelles sont les conditions à satisfaire pour qu'une autorité judiciaire ou policière puisse obtenir des données relatives aux abonnés auprès d'un fournisseur de services dans le cadre d'une enquête pénale ?**

La condition essentielle requise pour l'obtention d'informations relatives aux abonnés est qu'il y ait des motifs de croire qu'une personne a commis une infraction pénale.

En vertu de la législation australienne, la divulgation d'informations relatives aux abonnés est raisonnablement nécessaire aux fins de l'application du droit pénal.

Dans certains pays, d'autres conditions préalables s'appliquent : par exemple, que les informations ne puissent être obtenues par d'autres moyens ou qu'elles soient plus difficiles à obtenir (République tchèque), que les informations soient nécessaires à la réalisation des objectifs de la procédure pénale (Estonie), que l'intervention soit nécessaire et proportionnée (en Moldova, pour les cas n'impliquant pas d'infractions graves).

Les informations relatives aux abonnés peuvent être obtenues au moyen d'une requête officielle de la police dans les pays suivants :

- Autriche (pour les adresses IP statiques), Australie (uniquement les cadres habilités par le responsable de l'organe de répression), Bulgarie (uniquement les agents de rang supérieur), Danemark (pour les adresses IP statiques), Estonie, Finlande, Allemagne (tout organe de répression ou service de sécurité et de maintien de l'ordre), Japon (si les informations ne relèvent pas de « la confidentialité des communications »), Lituanie, Monténégro, Slovénie (pour les adresses IP statiques), Espagne (si les informations ne contreviennent pas à la confidentialité des communications).

Les informations relatives aux abonnés peuvent être obtenues sur ordonnance du procureur dans les pays suivants :

- Autriche (pour les adresses IP statiques), Croatie, Moldova (pour les cas impliquant une infraction grave), Portugal, Roumanie (si les informations relatives aux abonnés ne sont pas liées à une communication spécifique), Serbie, « l'ex-République yougoslave de Macédoine » et Etats-Unis<sup>8</sup>.

Les informations relatives aux abonnés ne peuvent être obtenues que sur ordonnance d'un juge dans les pays suivants :

- Azerbaïdjan, Bosnie-Herzégovine, République tchèque, Danemark (pour les adresses IP dynamiques), France, Japon (si les informations relèvent de la « confidentialité des communications »), Lettonie, Maurice, Moldova (pour les cas n'impliquant pas d'infractions graves), Roumanie (si les informations relatives aux abonnés sont liées à une communication spécifique, la loi sur la conservation des données s'applique), Slovénie (pour les adresses IP dynamiques), Espagne (si les informations contreviennent à la confidentialité des communications), Ukraine, Etats-Unis (une ordonnance du juge remplace une ordonnance de production des pièces).

Les Etats ont transmis les réponses suivantes :

<b>Etats</b>	<b>Autorité habilitée à ordonner la divulgation d'informations relatives aux abonnés</b>	<b>Conditions requises</b>
Australie	Un fonctionnaire habilité des services répressifs	Autorisation écrite du responsable d'un service répressif. Conditions pour la délivrance de l'autorisation : <ul style="list-style-type: none"> <li>- la divulgation est raisonnablement nécessaire pour l'application du droit pénal</li> <li>- la pertinence et l'utilité des <i>informations</i> ou des documents et la raison pour laquelle il est proposé d'en autoriser la divulgation ou l'utilisation.</li> </ul>
Autriche	Pour les adresses IP statiques : autorité de police  Pour les adresses IP dynamiques : ordonnance du ministère public	Pour les adresses IP statiques : il est nécessaire qu'il y ait des soupçons concrets d'infraction commise par une personne, indépendamment de sa gravité  Pour les adresses IP dynamiques : <ul style="list-style-type: none"> <li>- sur demande et ordre écrits ;</li> <li>- motifs de suspicion ;</li> <li>- restriction à l'obtention d'informations relatives aux abonnés si l'adresse IP est rattachée à plus de 10 personnes.</li> </ul>
Azerbaïdjan	Décision judiciaire	
Bosnie-Herzégovine	Pour les 3 entités et l'Etat : Ministère public ou agents habilités par celui-ci	Motif de suspicion qu'une personne a commis une infraction. Demande à la Cour
Bulgarie	Responsables des directions spécialisées, des directions régionales et des directions territoriales autonomes de l'agence	Demande écrite motivée adressée au président du tribunal de district. Eléments devant figurer dans la demande : <ul style="list-style-type: none"> <li>- le fondement juridique et la finalité de</li> </ul>

<sup>8</sup> Aux Etats-Unis, les informations seraient obtenues par une ordonnance de production de pièces, ce qui équivaldrait approximativement à une ordonnance du ministère public.

Etats	Autorité habilitée à ordonner la divulgation d'informations relatives aux abonnés	Conditions requises
	d'Etat pour la sécurité nationale	l'accès demandé ; - le numéro de référence du dossier, pour lequel l'accès est demandé ; - les données qui devraient figurer dans le rapport ; - la période concernée.
Croatie	Ministère public	Demande écrite du ministère public; Un délai pour la communication des données doit être fixé.
République tchèque	Juge principal ou juge proposé par le ministère public	Les demandes ne peuvent être faites que : - S'il s'agit d'infractions intentionnelles (passibles d'une peine d'au moins 3 ans) faisant l'objet de poursuites /ou de l'une des infractions expressément visées faisant l'objet de poursuites / ou d'une infraction que la République tchèque est tenue de poursuivre en application d'un traité international ; - Et si le but poursuivi (en se procurant les informations) ne peut être atteint par d'autres moyens ou serait en l'occurrence plus difficile à atteindre.
Danemark	Police (adresses IP statiques)  Décision judiciaire (adresses IP dynamiques)	Adresses IP statiques : demande émanant de la police  adresses IP dynamiques: - injonction de produire les informations demandées - seulement si les informations serviront ou pourraient servir d'éléments de preuve devant les tribunaux.
Estonie	Police ou autre organisme d'enquête	Sur demande. En veillant au respect du principe de proportionnalité.
Finlande	Police	Informations nécessaires à dans le cadre de fonctions policières.
France	Autorité judiciaire	Réquisition judiciaire établie par un officier de police; Réquisition mentionnant le cadre légal d'enquête ainsi que les infractions visées.
Allemagne	Autorités chargées : - d'engager des poursuites en cas d'infractions pénales ou de délits administratifs ; - de prévenir les menaces susceptibles de peser sur la sécurité et l'ordre publics ; - d'assurer la protection de la	Demande écrite émanant de l'une des autorités compétentes ; Obligation d'indiquer la finalité de la demande : aux fins de poursuivre des infractions ou des délits administratifs, de prévenir les menaces susceptibles de peser sur la sécurité ou l'ordre publics ou de permettre aux autorités énumérées à l'alinéa 3 d'exercer leurs

Etats	Autorité habilitée à ordonner la divulgation d'informations relatives aux abonnés	Conditions requises
	constitution aux niveaux de la fédération et des Länder.	responsabilités statutaires.
Japon	Demande émanant d'un organisme d'enquête	Prouver la nécessité d'atteindre l'objectif de l'enquête.
Lettonie	Juge	
Lituanie	Police ou autorité judiciaire	Demande officielle d'injonction de produire. La demande doit être envoyée à toute personne morale ou physique. La personne concernée est en possession des informations.
Maurice	Organisme d'enquête sur autorisation d'une ordonnance d'un juge	Demande d'autorisation d'un organisme d'enquête adressée au juge en chambre du conseil. Il existe des raisons de croire que les données concernées sont particulièrement sensibles aux risques de perte ou de modification.
Moldova	Juge d'instruction habilité  Dans le cas d'infractions graves : autorisation du ministère public	Autorisation du juge d'instruction lorsqu'il ne s'agit pas d'infractions graves.  Eléments devant figurer sur l'ordonnance : – 1) identification du fournisseur de service qui est en possession des données précisées au paragraphe (1) ou les a sous son contrôle ; – 2) identification de l'abonné, du propriétaire ou de l'utilisateur, s'ils sont connus, conditions motivant la prise de mesures spéciales d'enquête ; – 3) énoncé de l'obligation qu'a la personne ou le fournisseur d'accès de communiquer immédiatement et de manière confidentielle les informations demandées. – (3) les fournisseurs de service sont tenus de coopérer avec le ministère public pour l'exécution de l'ordonnance du procureur et de lui remettre immédiatement les informations demandées. – (4) les personnes appelées à coopérer avec le ministère public sont tenues de respecter la confidentialité des opérations menées. Tout manquement à cette obligation est passible de sanctions aux termes du Code pénal.
Monténégro	Police ou autorité judiciaire	Suspicion d'infraction pénale.
Norvège	Ministère public ou police	Demande émanant du ministère public ou de la police.

Etats	Autorité habilitée à ordonner la divulgation d'informations relatives aux abonnés	Conditions requises
Portugal	Ordonnance du procureur	Une ordonnance peut être émise si les informations recherchées sont nécessaires aux fins de « la collecte de preuves en vue d'établir la vérité » .
Roumanie	Décision de justice  S'il ne s'agit pas d'une communication spécifique, sur demande directe d'un procureur	
Serbie	Ministère public	Le ministère public, les pouvoirs publics et autres autorités ainsi que les personnes morales sont tenues d'agir avec diligence et de veiller à ce qu'aucune atteinte ne soit portée à l'honneur et à la réputation de la personne à laquelle les données se rapportent.
Slovaquie		
Slovénie	Police (pour les adresses IP statiques) Décision judiciaire (pour les adresses IP dynamiques)	Lettre officielle de la police. Raisons de suspecter un comportement délictueux.  Pour les adresses IP dynamiques, la réglementation en matière de conservation des données s'applique.
Espagne	Autorité judiciaire, ministère public, services répressifs	Les informations soumises à l'obligation de confidentialité des communications doivent faire l'objet d'une autorisation judiciaire. Les services répressifs peuvent avoir accès aux informations si elles ne contreviennent pas à la confidentialité des communications.  Mise en œuvre de la directive sur la conservation des données : – Demande de l'autorité judiciaire au moment de l'enquête relative à une infraction pénale grave.
« L'ex-République yougoslave de Macédoine »	Ministère public (au cours de la phase d'instruction et de l'enquête elle-même)	
Ukraine	Autorisation du juge	
Etats-Unis	Ordonnance de production de pièces, injonction du tribunal	Ordonnance de production de pièces pour obtenir les informations de base relatives à l'abonné. Ordonnance ou mandat du tribunal pour l'obtention de toute information détaillée complémentaire de non contenu relative à un abonné.

## **2.5 Conditions requises pour l'obtention de données relatives à un abonné pour une adresse IP particulière dans le cadre d'une enquête pénale spécifique**

**Question 5 : Quelles sont, spécifiquement, les conditions requises permettant aux services de police ou aux autorités judiciaires d'obtenir les données relatives à un abonné, pour une adresse IP particulière dans le cadre d'une enquête pénale spécifique ?**

Dans le cadre des enquêtes et des procédures pénales en matière de cybercriminalité, il est souvent nécessaire d'obtenir des informations auprès des fournisseurs d'accès internet (FAI) pour permettre :

- l'identification d'un abonné ayant utilisé une adresse IP définie à un moment précis ; ou
- l'identification de l'adresse IP utilisée par l'abonné d'un FAI dont l'identité est déjà connue.

Les données recherchées sont comparables à celles qui sont nécessaires pour identifier le titulaire d'un numéro de téléphone dans une enquête pénale.

La question qui se pose ici est de savoir si les Etats imposent des conditions particulières pour l'obtention d'informations relatives à un abonné utilisant une adresse IP spécifique.

Les réponses indiquent que la majorité des Parties ne fixent pas de conditions particulières. Parmi les exceptions, figurent par exemple :

- la Bosnie-Herzégovine : la police doit apporter au ministère public ou au tribunal la preuve que l'adresse IP est liée à une infraction pénale pour que lui soit délivrée l'autorisation d'obtenir les informations relatives à l'abonné.
- Japon : les adresses IP statiques ou dynamiques relatives à une communication spécifique sont généralement protégées au titre de la confidentialité des communications ; une ordonnance judiciaire est donc nécessaire pour obtenir les informations qui se rapportent à l'abonné.
- Roumanie : dans la mesure où l'adresse IP est un type de données nécessaires pour rechercher et identifier la source d'une communication ou d'une donnée indiquant la date, l'heure ou la durée d'une communication (articles 4 et 6 de la loi n°82/2012), les données relatives à un abonné concernant son adresse IP entrent dans le cadre d'une communication qui relève de la loi sur la conservation des données ; cela signifie que l'autorisation d'un juge est nécessaire à l'obtention des informations (art.152 NCP).

Comme indiqué plus haut, l'Autriche, le Danemark et la Slovénie imposent des conditions différentes pour l'obtention d'informations relatives aux abonnés selon qu'il s'agit d'adresses IP statiques ou dynamiques.

## **2.6 Catégories de données considérées comme des données relatives au trafic**

**Question 6 : Quelles sont, en vertu de votre droit interne, les catégories de données considérées comme des données relatives au trafic ? Veuillez fournir le texte correspondant.**

Au titre de l'article 1.d de la Convention de Budapest sur la cybercriminalité, les « données relatives au trafic » désignent :

« toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ».

Le paragraphe 30 du rapport explicatif précise les catégories de données considérées comme « données relatives au trafic » :

« La définition dresse la liste exhaustive des catégories de données relatives au trafic qui sont soumises à un régime particulier dans la Convention : origine de la communication, destination, itinéraire, heure (GMT), date, taille, durée et type du service sous-jacent. Ces catégories ne seront pas toujours toutes techniquement accessibles, susceptibles d'être produites par un fournisseur de service, ni nécessaires à l'enquête pénale. Par « origine », on entend un numéro de téléphone, une adresse IP ou un moyen similaire d'identifier un dispositif de communication auquel un prestataire de services fournit des services. La « destination » désigne une indication comparable concernant un dispositif de communication vers lequel des communications sont transmises. L'expression « type du service sous-jacent » renvoie au type du service utilisé au sein du réseau : transfert de fichiers, courrier électronique ou messagerie instantanée. »

Il ressort des réponses données par les Parties que la plupart d'entre elles définissent les données relatives au trafic dans leur législation et que beaucoup suivent la définition de l'article 1.d de la Convention de Budapest.

Dans certains Etats, la notion de « données relatives au trafic » est relativement vaste, celles-ci désignant les données collectées, traitées ou utilisées dans le cadre de la fourniture d'un service de télécommunications (Autriche, Monténégro, Lettonie, Serbie et d'autres).

La République tchèque utilise une classification des données relatives au trafic qui fait la distinction entre données relatives aux réseaux téléphoniques publics, aux réseaux publics de téléphonie mobile, aux communications électroniques, à l'accès mobile à internet, à l'accès au courrier électronique et à d'autres catégories.

L'Australie a répondu qu'elle n'établissait pas de distinction entre « données relatives aux abonnés » et « données relatives au trafic » mais seulement entre informations de contenu et de non-contenu. Toutes les informations dites de « non-contenu » sont considérées comme des « données de télécommunications » et traitées de la même manière.

Il convient de noter que la Directive de l'Union européenne sur la conservation des données<sup>9</sup> applique le même traitement aux données relatives au trafic qu'aux informations relatives aux abonnés (ainsi qu'aux données de localisation) et ne prévoit pas de conditions différentes pour l'obtention des différents types de données. Le champ d'application de la Directive est ainsi défini :

1. La présente directive a pour objectif d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

2. La présente directive s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques<sup>10</sup>.

La Directive dans sa version actuelle a toutefois été invalidée en avril 2014 par un arrêt de la Cour européenne de justice<sup>11</sup>.

Les Parties ont transmis les réponses suivantes :

Pays	Catégories de données considérées comme « données relatives au trafic »
Autriche	§ 92 (3) Z4 TKG 2003 "Verkehrsdaten": Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden.
Bosnie-Herzégovine	Article 3 point s) de la Décision sur les obligations spéciales des personnes physiques et morales : – Signaler les données contenues dans les télécommunications ou qui s'y rapportent, nécessaires au système de télécommunication par lequel elles sont transmises ; – Les informations sur la fourniture de services ou de systèmes de télécommunications à toute personne ou sur leur utilisation par toute personne, autre que le contenu des télécommunications, à l'exception des données relatives au trafic qu'elle contient, et – toute autre information en possession de l'opérateur de télécommunications qui fournit ou a fourni les services, telles que les informations relatives aux abonnés.

<sup>9</sup> Directive 2006/24/CE du Parlement et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>

<sup>10</sup> Soulignement ajouté.

<sup>11</sup> Arrêt dans les affaires jointes C-293/12 et C-594/12 Digital Rights Ireland et Seitlinger et autres

<http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>

La Cour a estimé que :

« La directive comporte une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel sans que cette ingérence soit limitée au strict nécessaire ».



Pays	Catégories de données considérées comme « données relatives au trafic »
Bulgarie	<p>Article 248 de la loi sur les communications électroniques</p> <ul style="list-style-type: none"> <li>- données nécessaires à la fourniture de services de communications électroniques, à la facturation, à l'émission de factures pour les abonnés et à l'établissement de leur authenticité, notamment : <ul style="list-style-type: none"> <li>a) le numéro de l'appelant et de l'utilisateur final appelé, le numéro de carte bancaire pour les paiements en ligne ;</li> <li>b) le début et la fin de l'appel, déterminés par la date et l'heure à la seconde près, si les conditions techniques le permettent, et/ou en cas de transfert de données - le volume de données transférées à des fins de facturation ;</li> <li>c) le type de service fourni ;</li> <li>d) les points d'interconnexion de l'appel, le début et la fin de leur utilisation, déterminés par la date et l'heure à la seconde près, si les conditions techniques le permettent ;</li> <li>e) détails sur le type de connexion ou les zones, horaires et géographiques, nécessaires pour déterminer la valeur du service ;</li> <li>f) la localisation de l'utilisateur d'un service, fourni par un réseau mobile, y compris la fourniture de services d'itinérance ("roaming") ;</li> </ul> </li> </ul>
Croatie	<p>Loi sur les communications électroniques (article 110, paragraphe 1):</p> <ul style="list-style-type: none"> <li>- données nécessaires pour retrouver et identifier la source d'une communication;</li> <li>- données nécessaires pour identifier la destination d'une communication;</li> <li>- données nécessaires pour déterminer la date, l'heure et la durée d'une communication;</li> <li>- données nécessaires pour déterminer le type de communication;</li> <li>- données nécessaires pour identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel ;</li> <li>- données nécessaires pour localiser le matériel de communication mobile.</li> </ul>
République tchèque	<p>Article 2 du règlement n° 357/2012 sur l'archivage, le transfert et la suppression des données d'exploitation et de localisation :</p> <ul style="list-style-type: none"> <li>- Type de connexion,</li> <li>- Numéro de téléphone ou d'identification de l'utilisateur,</li> <li>- Identifiant du compte de l'utilisateur,</li> <li>- Adresse MAC de l'appareil de l'utilisateur,</li> <li>- Date et heure de début et de fin de la connexion internet,</li> <li>- Indication du point d'accès de la connexion internet sans fil,</li> <li>- Adresse IP et numéro de port qui ont été utilisés pour la connexion internet ;</li> </ul>
Estonie	<p>Article 111<sup>1</sup> (3) de la loi sur les communications électroniques :</p> <ul style="list-style-type: none"> <li>- Les identifiants de l'utilisateur attribués par l'opérateur de communications ;</li> <li>- Le numéro d'identifiant de l'utilisateur et le numéro de téléphone de toute communication entrante du téléphone ou du réseau de téléphonie mobile ;</li> <li>- Les nom et adresse de l'abonné auquel une adresse IP, un identifiant ou un numéro de téléphone a été attribué au moment de la communication ;</li> <li>- Le numéro d'identifiant de l'utilisateur ou le numéro de téléphone du destinataire prévu d'un appel téléphonique par internet ;</li> <li>- Les nom, adresse et identifiant de l'abonné qui est le destinataire prévu dans le cas de services de courrier électronique et de téléphonie par internet ;</li> <li>- La date et l'heure de début et de fin de la session internet, dans un fuseau horaire déterminé, ainsi que l'adresse IP attribuée à l'utilisateur par le fournisseur d'accès à l'internet et son numéro d'identifiant ;</li> <li>- La date et l'heure de l'ouverture et de la fermeture du service de courrier électronique du service de courrier électronique ou de téléphonie par l'internet dans un fuseau horaire déterminé</li> </ul>

Pays	Catégories de données considérées comme « données relatives au trafic »
	<ul style="list-style-type: none"> <li>- Le service internet utilisé dans le cas de services de courrier électronique et de téléphonie par internet ;</li> <li>- Le numéro de l'appelant en cas d'appel commuté à internet ;</li> <li>- la ligne d'abonné numérique (DSL) ou tout autre point terminal de l'auteur de la communication.</li> </ul>
Finlande	<p>La surveillance des données relatives au trafic est régie par le chapitre 10 de la loi sur les mesures de contrainte (806/2011). L'article 6 régit la surveillance des télécommunications (et non l'interception, qui est une question différente), par exemple, l'obtention d'informations d'identification concernant un message qui a été envoyé depuis une adresse à distance. Aux termes de ladite disposition « la surveillance des données relatives au trafic désigne l'obtention de données d'identification concernant un message qui a été envoyé ou reçu par une adresse réseau ou un équipement terminal connecté à un réseau de télécommunications visé à l'article 3, l'obtention de données de localisation concernant l'adresse réseau ou l'équipement terminal ou le blocage temporaire de l'utilisation de l'adresse réseau ou de l'équipement terminal. Les données d'identification désignent les données visées à l'article 2, paragraphe 8 de la loi sur la protection de la vie privée dans les communications électroniques (516/2004) qui peuvent être associées à un abonné ou un utilisateur et qui sont traitées dans des réseaux de télécommunications en vue de transmettre ou diffuser des messages ou de les conserver.</p> <p>Au titre de la disposition de la loi 516/2004 susmentionnée « les données d'identification désignent les données qui peuvent être associées à un abonné ou un utilisateur et qui sont traitées dans des réseaux de communications aux fins de transmettre, distribuer ou fournir des messages ». A ces fins, l'adresse IP est considérée comme une information d'identification.</p>
France	<p>Article L34-1 du Code des Postes et des Communications Electroniques, introduit par l'article 20 de la loi 2003-239 du 18 mars 2003 sur la sécurité intérieure :</p> <ul style="list-style-type: none"> <li>- données techniques liées à l'utilisation des réseaux qu'il s'agisse de communications téléphoniques, de courriers électroniques, d'accès à un site internet, de SMS, ou de services de messagerie multimédia (MMS) et permettent d'identifier les interlocuteurs, leur localisation et la durée de leur communication.</li> </ul>
Allemagne	<p>Article 3 n° 30 de la loi sur les télécommunications :</p> <ul style="list-style-type: none"> <li>- données collectées, traitées ou utilisées dans le cadre de la fourniture d'un service de télécommunications.</li> </ul>
Japon	<p>L'origine, la destination, l'heure et toute autre donnée relative au trafic de la communication électronique.</p>
Lettonie	<p>Article 1.1 (29) de la loi sur les communications électroniques :</p> <ul style="list-style-type: none"> <li>- toutes les informations ou données qui sont traitées en vue de transmettre des informations par un réseau de communications électroniques ou d'émettre des factures et calculer le montant des paiements, à l'exception du contenu effectif des informations transmises.</li> </ul>
Lituanie	<p>Article 3 paragraphe 57 de la loi sur les communications électroniques :</p> <ul style="list-style-type: none"> <li>- toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques et/ou de sa facturation.</li> </ul>
Maurice	<p>Partie 1, article 2, « réseau de télécommunications (...) » Clause (d) de la loi sur la protection des données de 2001 :</p> <ul style="list-style-type: none"> <li>- données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la</li> </ul>

Pays	Catégories de données considérées comme « données relatives au trafic »
	communication ou le type de service sous-jacent.
Moldova	<p>Article 2 de la loi n° 20 du 03.02.2009 sur la prévention et la lutte contre la cybercriminalité :</p> <ul style="list-style-type: none"> <li>- toutes les données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent;</li> </ul>
Monténégro	<p>Loi sur les communications électroniques :</p> <ul style="list-style-type: none"> <li>- « données traitées en vue de la fourniture de services de communications électroniques ou de leur facturation »</li> </ul>
Portugal	<p>Article 2, c) de la loi sur la cybercriminalité (loi n° 109/2009, du 15 septembre):</p> <ul style="list-style-type: none"> <li>- données informatiques ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ;</li> <li>- (...)</li> </ul>
Roumanie	<p>Loi n° 82/2012 (loi sur la conservation des données) :</p> <ul style="list-style-type: none"> <li>- la définition générale des données englobe les données relatives au trafic ainsi qu'à la localisation et les informations nécessaires à l'identification d'un abonné ou d'un utilisateur.</li> </ul> <p>Loi n° 506/2004 article 2 alinéa b) (loi n° 506/2004 sur la protection des données à caractère personnel à l'égard de leur traitement dans le cadre d'une communication électronique) :</p> <ul style="list-style-type: none"> <li>- toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques et/ou de sa facturation.</li> </ul> <p>Loi n° 161/2003 article 35 alinéa f) (loi transposant la CC de 2001):</p> <ul style="list-style-type: none"> <li>- toutes les données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ;</li> </ul>
Slovénie	<p>Loi sur les communications électroniques (article 3, définition n° 25):</p> <ul style="list-style-type: none"> <li>- routage, durée, moment ou volume d'une communication,</li> <li>- le protocole de référence,</li> <li>- l'emplacement des équipements terminaux de l'expéditeur ou du destinataire,</li> <li>- le réseau de départ ou d'arrivée de la communication,</li> <li>- le début, la fin ou la durée d'une connexion</li> <li>- le format dans lequel le message a été acheminé par le réseau.</li> </ul>
Espagne	<p>Article 64.a) du décret royal 424/2005 du 15 avril :</p> <ul style="list-style-type: none"> <li>- toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation.</li> </ul>
« L'ex-République yougoslave de Macédoine »	<p>Aux termes des dispositions de l'article 122, paragraphe 27 du Code pénal, les données relatives au trafic sont définies comme suit :</p> <ul style="list-style-type: none"> <li>- les données informatiques désignent toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction.</li> </ul>

Pays	Catégories de données considérées comme « données relatives au trafic »
Ukraine	– ensemble des signaux transmis par des moyens techniques par des opérateurs et des fournisseurs de services de télécommunications à intervalles de temps définis, y compris les informations relatives à l'utilisateur et/ ou les renseignements exclusifs.
Etats-Unis	18 U.S.C. § 2703(c)(1): – informations de « non contenu » : « renseignements ou toute autre information appartenant à un abonné ou à un client de ce service (n'incluant pas le contenu des communications) ». – Cette catégorie englobe les informations concernant les adresses des autres personnes avec lesquelles l'abonné communique, y compris les adresses de courrier électronique et les adresses IP.

## 2.7 Conditions requises pour l'obtention de données relatives au trafic auprès d'un fournisseur de services dans le cadre d'une enquête pénale

### Question 7 : Quelles sont les conditions requises pour permettre aux services de police ou aux autorités judiciaires d'obtenir des informations relatives au trafic auprès d'un fournisseur de services dans le cadre d'une enquête pénale ?

Certaines Parties n'établissent pas de distinction entre « données relatives au trafic » et « données relatives aux abonnés » et concernant les conditions nécessaires à leur obtention : Australie, Bosnie-Herzégovine, Bulgarie, République tchèque, France, Lituanie, Slovaquie et Ukraine.

En revanche, la plupart des Parties disposent de procédures spécifiques pour l'obtention de données relatives au trafic :

Etat	Autorité habilitée à obtenir les données relatives au trafic	Conditions requises
Autriche	Ministère public	§ 135 Abs 2 StPO ordonnance écrite spécifiant les motivations du ministère public
Croatie	Pour les utilisateurs inscrits : Services de police sur ordonnance du juge d'instruction  Pour les utilisateurs non inscrits : Agent de police	Pour les utilisateurs inscrits, Code de procédure pénale (Article 339a): – motifs de suspecter que l'utilisateur inscrit a commis une infraction pénale – demande émanant des services de police sur ordonnance du juge d'instruction – aux fins de la collecte d'éléments de preuve  Pour les utilisateurs non inscrits, article 68 de la loi sur les activités et compétences de la police : – Aux fins de la prévention de la criminalité et de la détection des infractions pénales.
Danemark	En cas d'atteinte à la confidentialité des communications, y compris les données relatives au trafic :	Article 781 de la loi sur l'administration de la justice : – Décision judiciaire motivée par des raisons concrètes laissant présumer que les moyens de

<b>Etat</b>	<b>Autorité habilitée à obtenir les données relatives au trafic</b>	<b>Conditions requises</b>
	Services de police / autorité judiciaire	communication en question sont utilisés pour acheminer des messages dont le suspect est l'expéditeur ou le destinataire et que l'atteinte est considérée comme essentielle à une enquête concernant une infraction grave.
Estonie	Organisme d'enquête sur autorisation du ministère public	paragraphe 90 du Code de procédure pénale : – L'autorisation doit indiquer les dates de la période concernée pour lesquelles la demande d'informations est autorisée.
Finlande	Autorisation judiciaire	Chapitre 10, articles 6 et 9 de la loi sur les mesures de contrainte.
Allemagne	Services répressifs	Article 100g du Code de procédure pénale : – Grounds for suspicion that a person has committed a criminal offence of substantial significance or a criminal offence by means of telecommunication. Order by a court or - in exigent circumstances - the public prosecution office.
Japon	Organisme d'enquête	Avis de saisie délivré par un juge
Lettonie	Police ou autorité judiciaire	Sur demande auprès du fournisseur de services
Maurice	Injonction de conservation: Commissaire à la protection des données  Collecte en temps réel de données relatives au trafic : Organisme d'enquête	Injonction de conservation : – Sur approbation du juge en chambre du conseil  Collecte en temps réel de données relatives au trafic : – Motifs raisonnables ; – Sous réserve des instructions du juge en chambre du conseil.
Moldova	En cas d'infraction grave : Juge  Pour les infractions moins graves : Ministère public sur autorisation du juge d'instruction	En cas d'infraction grave : Collecte d'informations auprès des fournisseurs de services de communications électroniques (articles 132/1 et 134 du Code de procédure pénale) : – Seul moyen d'engager des poursuites pénales ; – Motifs raisonnables de suspecter une infraction grave ; – Les mesures sont nécessaires et proportionnées.  Pour les infractions moins graves : article 301 du Code de procédure pénale.
Monténégro		Eléments de l'infraction pénale.
Norvège	Ministère public	Le ministère public a besoin d'une injonction de produire délivrée par le tribunal de district.
Portugal	Autorisation judiciaire	Articles 187 et 189 du Code de procédure pénale : – Cette autorisation peut être délivrée s'il y a des raisons de croire que cette démarche est essentielle pour établir la vérité ou que les preuves seraient autrement impossibles à recueillir ou très difficiles à obtenir par d'autres

Etat	Autorité habilitée à obtenir les données relatives au trafic	Conditions requises
		moyens.
Roumanie	Autorisation judiciaire	Conditions telles que définies aux termes de la loi sur la conservation des données.
Serbie	Tribunal	Ordonnance judiciaire.
Slovénie	Police	<ul style="list-style-type: none"> <li>- Motifs de suspicion d'un acte criminel</li> <li>- Ordonnance judiciaire</li> </ul>
Espagne	Autorisation judiciaire	Suspicion d'une infraction grave (loi transposant la directive sur la conservation des données)
« L'ex-République yougoslave de Macédoine »	Ministère public	
Etats-Unis	Tribunal	<p>18 U.S.C. § 2703(c)(1), (d).</p> <p>Mandat de perquisition</p> <ul style="list-style-type: none"> <li>- Ordonnance judiciaire délivrée sur présentation « de faits spécifiques et précis » démontrant que les informations recherchées sont « pertinentes et déterminantes pour une enquête pénale en cours ».</li> </ul>

### 3 Conclusion

L'identification de l'abonné auquel se rapporte une adresse IP utilisée est l'information la plus souvent recherchée dans le cadre des enquêtes pénales nationales et internationales en matière de cybercriminalité et de preuve électronique. Elle est, la plupart du temps, déterminante pour établir la vérité : sans cette information préliminaire, il est bien souvent impossible de poursuivre l'enquête.

La Convention de Budapest établit une distinction entre les données relatives au trafic et les données relatives aux abonnés ; des réglementations différentes peuvent donc s'appliquer en ce qui concerne l'accès aux unes et aux autres. Les adresses IP peuvent être considérées comme étant des données relatives aux abonnés – par opposition aux données relatives au trafic – dès lors que l'objectif est d'identifier un abonné utilisant une adresse IP. On peut partir du principe que, dans la plupart des Etats parties, les adresses IP doivent être considérées comme des données à caractère personnel dans ce contexte précis.

La plupart des Parties qui ont répondu au questionnaire font en effet la différence, dans leurs définitions et leurs concepts, entre « données relatives aux abonnés » et « données relatives au trafic ».

Les conditions requises pour l'obtention des informations relatives aux abonnés varient toutefois selon les pays :

- Dans la plupart des Parties ayant répondu au questionnaire, il apparaît que les conditions requises pour l'obtention d'informations relatives aux abonnés sont semblables ou similaires à celles requises pour l'obtention de données relatives au trafic, notamment si les données relatives aux abonnés sont associées à une adresse IP dynamique. Dans plus de la moitié des Parties en question, une autorisation judiciaire est nécessaire pour obtenir des informations relatives aux abonnés ; dans d'autres, le ministère public ou un haut responsable des services répressifs habilité peut ordonner la production de ces informations.
- Dans d'autres Parties, les conditions requises pour l'obtention des informations relatives aux abonnés sont moins exigeantes que celles requises pour les données relatives au trafic et la production d'informations relatives aux abonnés peut être ordonnée par la police ou le ministère public.

En conclusion :

- La plupart des Parties font la différence entre « données relatives aux abonnés » et « données relatives au trafic » ;
- Dans certains pays, l'atteinte aux droits fondamentaux est considérée comme étant nettement différente selon qu'il s'agit de l'obtention de données relatives aux abonnés, y compris concernant une adresse IP, dans le cadre d'une enquête pénale spécifique d'une part, ou de données relatives au trafic d'autre part ;
- En conséquence, dans ces pays, des règles différentes devraient-elles s'appliquer pour l'obtention des informations en question ;
- Les conditions requises pour l'obtention des données relatives aux abonnés sont, à l'heure actuelle, relativement variées ;
- Néanmoins, une plus grande harmonisation des règles en matière d'obtention des informations relatives aux abonnés faciliterait la coopération internationale.

Il est recommandé au T-CY :

- de favoriser une plus grande harmonisation entre les Parties concernant les conditions, les règles et les procédures en matière d'obtention des données relatives aux abonnés ;
  - d'encourager les Parties à tenir compte des observations du présent rapport lors de la refonte de leur législation interne.
-



## 4 Appendix: Compilation of replies

### 4.1 Australia

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

No, IP address is not defined in relevant Australian laws.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

An IP address can be considered personal data in certain circumstances.

The definition of personal information is found in subsection 6(1) of the *Privacy Act 1988* as follows:

**personal information** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- (a) whether the information or opinion is true or not; and
- (b) whether the information or opinion is recorded in a material form or not.

Whether an individual is 'reasonably identifiable' from particular information will depend on considerations that include, relevantly:

- other information either held by or available to the entity that holds the information,
- whether it is possible for the individual or entity that holds the information to identify the individual, using available resources (including other information available to that individual or entity). Where it may be possible to identify an individual using available resources, the practicability, including the time and cost involved, will be relevant to deciding whether an individual is 'reasonably identifiable'

Whether a person is 'reasonably identifiable' is an objective test that has practical regard to the context in which the issue arises. Even though it may be technically possible to identify an individual from information, if doing so is so impractical that there is almost no likelihood of it occurring, the information would not generally be regarded as 'personal information'. An individual may not be reasonably identifiable if the steps required to do so are excessively time-consuming or costly in all the circumstances. Further, the Office of the Australian Information Commissioner's view (the Australian privacy regulator) is that, where it is unclear whether an individual is 'reasonably identifiable', an entity should err on the side of caution and treat the information as personal information.

It is reasonable to conclude that an IP address would be considered personal information where it is held by an entity which would have access to other information which would allow them to identify the owner/user of that IP address. This is sometimes referred to as the 'mosaic effect', and would be particularly relevant to a communications provider or telecommunications company in this context, as they would have relatively easy access to other information associated with the IP address.

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

Australian law does not distinguish between subscriber information and traffic information. The *Telecommunications (Interception and Access) Act 1979* (the TIA Act) makes a distinction between the content of communications and non-content information about communications. However, there are no further distinctions or categories of non-content information. All non-content data ("information or documents") are treated equally. This broad category of information is called "telecommunications data".

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

When making an authorisation to disclose telecommunications data (for example, an IP address), authorised officers of law enforcement agencies must satisfy themselves that that "the disclosure is reasonably necessary for the enforcement of the criminal law" and whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to the likely relevance and usefulness of the information or documents and the reason why the disclosure or use concerned is proposed to be authorised.

The power to authorise the disclosure of telecommunications data is limited to certain management-level officers who have been designated in writing by the head of their law enforcement agency.

Those requirements are in sections 5AB, 179 and 180F of the TIA Act. Section 180F was inserted into the TIA Act in order for Australia to comply with the Budapest Convention.

Section 5AB:

Authorised officers

(1) The head (however described) of an enforcement agency may, by writing, authorise a management office or management position in the enforcement agency for the purposes of... the definition of authorised officer.

Section 178:

Authorisations for access to existing information or documents--enforcement of the criminal law

(1) Sections 276, 277 and 278 of the Telecommunications Act 1997 do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under subsection (2).

(2) An authorised officer of an enforcement agency may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

(3) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law.

Section 180F:

Authorised officers to consider privacy

Before making an authorisation under Division 4 or 4A in relation to the disclosure or use of information or documents, the authorised officer considering making the authorisation must have regard to whether any interference with the privacy of any person or

persons that may result from the disclosure or use is justifiable, having regard to the following matters:

(a) the likely relevance and usefulness of the information or documents;

(b) the reason why the disclosure or use concerned is proposed to be authorised.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

There are no further requirements for obtaining IP address information beyond the requirements in sections 178 and 180F as set out in the answer to question 4.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

[same answer as for question 3]

Australian law does not distinguish between subscriber information and traffic information. The *Telecommunications (Interception and Access) Act 1979* (the TIA Act) makes a distinction between the content of communications and non-content information about communications. However, there are no further distinctions or categories of non-content information. All non-content data (“information or documents”) are treated equally. This broad category of information is called “telecommunications data”.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

[same answer as for question 4]

When making an authorisation to disclose telecommunications data (for example, an IP address), authorised officers of law enforcement agencies must satisfy themselves that that “the disclosure is reasonably necessary for the enforcement of the criminal law” and whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to the likely relevance and usefulness of the information or documents and the reason why the disclosure or use concerned is proposed to be authorised.

The power to authorise the disclosure of telecommunications data is limited to certain management-level officers who have been designated in writing by the head of their law enforcement agency.

Those requirements are in sections 5AB, 179 and 180F of the TIA Act. Section 180F was inserted into the TIA Act in order for Australia to comply with the Budapest Convention.

Section 5AB:

Authorised officers

(1) The head (however described) of an enforcement agency may, by writing, authorise a management office or management position in the enforcement agency for the purposes of... the definition of authorised officer.

Section 178:

Authorisations for access to existing information or documents--enforcement of the criminal law

(1) Sections 276, 277 and 278 of the Telecommunications Act 1997 do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under subsection (2).

(2) An authorised officer of an enforcement agency may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

(3) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law.

Section 180F:

Authorised officers to consider privacy

Before making an authorisation under Division 4 or 4A in relation to the disclosure or use of information or documents, the authorised officer considering making the authorisation must have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to the following matters:

\_\_\_\_\_ (a) the likely relevance and usefulness of the information or documents;

\_\_\_\_\_ (b) the reason why the disclosure or use concerned is proposed to be authorised.

## 4.2 Austria

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

Yes, the term "public IP address" is defined. However, the text can only be provided in German language.

§ 92 (3) Z 16 Telekommunikationsgesetz (TKG) 2003

„öffentliche IP-Adresse“: eine einmalige numerische Adresse aus einem Adressblock, der durch die Internet Assigned Numbers Authority (IANA) oder durch eine regionale Vergabestelle (Regional Internet Registries) einem Anbieter eines Internet-Zugangsdienstes zur Zuteilung von Adressen an seine Kunden zugewiesen wurde, die einen Rechner im Internet eindeutig identifiziert und im Internet geroutet werden kann.

Öffentliche IP-Adressen sind Zugangsdaten im Sinne des § 92 Abs. 3 Z

4a. Wenn eine konkrete öffentliche IP-Adresse einem Teilnehmer für die Dauer des Vertrages zur ausschließlichen Nutzung zugewiesen ist, handelt es sich zugleich um ein Stammdatum im Sinne des § 92 Abs. 3 Z 3;

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

Yes, an IP address is considered to be personal data.

§ 92 (3) Z 16 letzter Satz TKG 2003

Wenn eine konkrete öffentliche IP-Adresse einem Teilnehmer für die Dauer des Vertrages zur ausschließlichen Nutzung zugewiesen ist, handelt es sich zugleich um ein Stammdatum im Sinne des § 92 Abs. 3 Z 3;

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

The following categories of data are to be considered subscriber information: name, academic degree, place of residence, user number or other such numbers, information on the type and content of the contract, credit-rating.

The text of the respective law can only be provided in German language.

§ 92 (3) Z 3 TKG 2003

„Stammdaten“: alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:

- a) Name (Familiename und Vorname bei natürlichen Personen, Name bzw. Bezeichnung bei juristischen Personen),
- b) akademischer Grad bei natürlichen Personen,
- c) Anschrift (Wohnadresse bei natürlichen Personen, Sitz bzw. Rechnungsadresse bei juristischen Personen),
- d) Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,
- e) Information über Art und Inhalt des Vertragsverhältnisses,
- f) Bonität

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

The Service Provider has to provide subscriber information of a static IP address to the police or judicial authority according to § 76a CPC in case of a criminal investigation if there is a concrete suspicion of a crime (regardless of its severity) committed by a person. A request from a police authority will be sufficient.

Subscriber information of a dynamic IP address has to be provided only upon a written and order of the public prosecution service in charge, which has to state the reasons, as well.

In urgent cases, also oral orders followed by a written order will be accepted.

However, law enforcement authorities may not obtain subscriber information (Z 1), if the IP-address may refer to more than 10 people (NAT/PAT addresses).

The respective Austrian Law can only be provided in German language:

§ 76a CPC

(1) Anbieter von Kommunikationsdiensten sind auf Ersuchen von kriminalpolizeilichen Behörden, Staatsanwaltschaften und Gerichten, die sich auf die Aufklärung des konkreten Verdachts einer Straftat einer bestimmten Person beziehen, zur Auskunft über Stammdaten eines Teilnehmers (§ 90 Abs. 7 TKG) verpflichtet.

(2) Gleiches gilt auf Anordnung der Staatsanwaltschaft (§ 102) für die Auskunft über folgende in § 99 Abs. 5 Z 2 TKG erwähnte Daten des Inhabers der betroffenen technischen Einrichtung:

1. Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP- Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war, es sei denn, dass diese Zuordnung eine größere Zahl von Teilnehmern erfassen würde
2. die bei Verwendung von E-Mail Diensten dem Teilnehmer zugewiesene Teilnehmerkennung
3. Name und Anschrift des Teilnehmers, dem eine E-Mail-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, und
4. die E-Mail-Adresse und die öffentliche IP-Adresse des Absenders einer E-Mail.

Die Bestimmungen der §§ 138 Abs. 5 und 139 gelten für diese Anordnung sinngemäß.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

See answer to question 4.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

The definition can only be provided in German language.

§ 92 (3) Z4 TKG 2003

“Verkehrsdaten”: Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

A written order which states the reasons and is authorized by the court has to be submitted has to be issued by the public prosecution service. In general, there are no special requirements with regard to the degree of suspicion. Suspicion based on probable cause suffices. Only in case of a hijacking a strong suspicion has to be provided.

The relevant Austrian stipulations can only be provided in German language.

Law enforcement authorities may not obtain any traffic data that has been retained for more than six months prior to the request.

In case of access which is stored according to data retention provisions approval of the Austrian Ombudsman has to be sought, as well.

§ 135 Abs 2 StPO

Auskunft über Daten einer Nachrichtenübermittlung (§ 134 Z 2 StPO) ist zulässig,

1. wenn und solange der dringende Verdacht besteht, dass eine von der Auskunft betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird,
2. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt, oder
3. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.
4. wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.

### 4.3 Azerbaijan

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

The term "IP address" is not defined in Azerbaijan legislation

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

-

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

-

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

We use Law of the Azerbaijani Republic «On operative-investigative activities», article 10-th which gives the opportunity to request this information from service providers, on the basis of article 445 of the criminal procedure code of AR under a court decision.

445.1.3. collect information from technical communication channels and other technical means;

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

We use Law of the Azerbaijani Republic «On operative-investigative activities», article 10-th which gives the opportunity to request this information from service providers, on the basis of article 445 of the criminal procedure code of AR under a court decision.

445.1.3. collect information from technical communication channels and other technical means;

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

-

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

We use Law of the Azerbaijani Republic «On operative-investigative activities», article 10-th which gives the opportunity to request this information from service providers, on the basis of article 445 of the criminal procedure code of AR under a court decision.

445.1.3. collect information from technical communication channels and other technical means;

There are no clear rules and procedures for obtain traffic data in the criminal code. In our activities we rely on bilateral memoranda about cooperation with service providers, concluded on the basis of article 39 of the «Law on Telecommunications».



#### 4.4 Bosnia and Herzegovina

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

The term "IP" address is not defined in the applicable criminal and criminal procedure codes of Bosnia and Herzegovina (Criminal Code of Bosnia and Herzegovina, the Criminal Procedure Code of Bosnia and Herzegovina, Criminal Code of the Republic of Srpska, Criminal Procedure Code of the Republic of Srpska, Criminal Code of the Federation of Bosnia and Herzegovina, Criminal Procedure Code of the Federation of Bosnia and Herzegovina, Criminal Code of Brcko District of Bosnia and Herzegovina, Criminal Procedure Code of Brcko District of Bosnia and Herzegovina).

The Criminal Procedure Code of Brcko District of Bosnia and Herzegovina (Official Gazette of Brcko District of BiH, No. 48/04, 6/05, 14/07, 19/07, 21/07, 2/08, 17/09 and 9/13), in Article 20 under Item s) defines the term "Telecommunication address". The text of this item of the aforementioned Article reads: "Telecommunication address" is every phone number, landline or mobile or email or web address owned or used a particular person.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

The Law on Protection of Personal Data of Bosnia and Herzegovina (BiH Official Gazette, No. 49/06, 76/11 and 89 /11) does not specifically define "IP" address, but generally Article 3 provides for the definition of personal data and the holder of personal data, which read:

"Personal data means any information relating to a natural person who is identified or whose identity can be established;

The holder of personal data is a natural person whose identity can be determined or identified."

Police of Brcko District of Bosnia and Herzegovina in its reply stated that in practice so far they have not had cases in where it was necessary to discuss whether the IP address is considered personal information so they are not able to provide a reliable answer. Considering the provisions of the Law on Protection of Personal Data, BiH Brcko District Police believes that the IP address does not represent personal information as on the grounds of the same address it is not possible to identify a specific person. As an example, they state that a user of a specified IP address can be an institution that has employed more than one person or a dynamic IP address that is not related to just one person.

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

The term information on the user is not defined in the criminal code in Bosnia and Herzegovina (Criminal Code of Bosnia and Herzegovina, the Criminal Procedure Code of Bosnia and Herzegovina, Criminal Code of the Republic of Srpska, Criminal Procedure Code of the Republic of Srpska, Criminal Code of the Federation of Bosnia and Herzegovina, Criminal Procedure Code of the Federation of Bosnia and Herzegovina, Criminal Code of Brcko District of Bosnia and Herzegovina, Criminal Procedure Code of Brcko District of Bosnia and Herzegovina).

Article 2 of the Law on Communications defines the database directory of phone numbers, and the same law does not provide defined information for Internet users.

Information on users as defined by the term "Subscriber Information" as prescribed in Article 3 Item m) Decisions of special obligations of legal and natural persons who provide telecommunications services, administer telecommunications networks and perform telecommunications services, in terms of providing and maintaining capacity that would allow authorized agencies to carry out lawful interception of telecommunications , as well as the capacity for storing and providing data of telecommunications (Decision of the Council of Ministers No. 258/06 ) , which reads: "*Subscriber Information*" is the name and address of the legal, physical, or other person to whom the telecommunication address is registered.

According to the Federal Ministry of Internal Affairs, this category also includes the data contained in the Agreement on the Subscription Relation of Users and ISP.

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

During a criminal investigation by police, the following conditions must be fulfilled so that the judicial authority could obtain user information related to internet service providers are defined by the following legal provisions:

Article 72a of the Criminal Procedure Code of Bosnia and Herzegovina

Order to the telecommunications operator

(1) If there are grounds for suspicion that a person has committed a criminal offence, on the basis of motion of the Prosecutor or officials authorized by the Prosecutor, the Court may issue an order to a telecommunications operator or another legal person performing telecommunications services to deliver information concerning the use of telecommunications services by that person, if such information could be used as evidence in the criminal proceedings or in collecting information that could be useful to the criminal proceedings.

Article 137 paragraph 1) of the Code of Criminal Procedure of the Republic of Srpska:

(1) If there are grounds for suspicion that a person has committed a criminal offence, on the basis of motion of the Prosecutor or officials authorized by the Prosecutor, the Court may issue an order to a telecommunications operator or another legal person performing telecommunications services to deliver information concerning the use of telecommunications services by that person, if such information could be used as evidence in the criminal proceedings or in collecting information that could be useful to the criminal proceedings.

Article 86a. Criminal Procedure Code of the Federation of Bosnia and Herzegovina:

Order to the telecommunications operator

(1) If there are grounds for suspicion that a person has committed a criminal offence, on the basis of motion of the Prosecutor or officials authorized by the Prosecutor, the Court may issue an order to a telecommunications operator or another legal person performing telecommunications services to deliver information concerning the use of telecommunications services by that person, if such information could be used as evidence in the criminal proceedings or in collecting information that could be useful to the criminal proceedings.

Article 72a. Paragraph (1) of the Criminal Procedure Code of District Brcko of BiH:

(1) If there are grounds for suspicion that a person has committed a criminal offence, on the basis of motion of the Prosecutor or officials authorized by the Prosecutor, the Court may issue an order to a telecommunications operator or another legal person performing telecommunications services to deliver information concerning the use of telecommunications services by that person, if such information could be used as evidence in the criminal proceedings or in collecting information that could be useful to the criminal proceedings.

Paragraph (4) of the same Article reads as follows:

“Telecommunications operators or other legal persons who provide telecommunications services shall enable the Prosecutor and competent authorities to enforce the measures referred to in Paragraph (1) of this Article.”

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

The conditions to be met in order to facilitate a criminal investigation by police or judicial authority by providing information about the user regarding the “IP” address as defined by the applicable provisions of the Criminal Procedure Code (as quoted in response to the previous question).

As more concrete conditions, the State Investigation and Protection Agency, and the Federal Ministry of the Interior stated the following:

- a. If in the course of the investigation it has been established that a particular IP address had been used for committing the criminal offense;
- b. If the operational work of police leads to the IP addresses of the offender, and the same can be used for detecting and locating that person;
- c. They must provide concrete evidence that in addition to the IP address indicate execution of a criminal offense.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

Data on traffic data are not defined in the Criminal Code in Bosnia and Herzegovina (Criminal Code of Bosnia and Herzegovina, the Criminal Procedure Code of Bosnia and Herzegovina, Criminal Code of the Republic of Srpska, Criminal Procedure Code of the Republic of Srpska, Criminal Code of the Federation of Bosnia and Herzegovina, Criminal Procedure Code of the Federation of Bosnia and Herzegovina, Criminal Code of Brcko District of Bosnia and Herzegovina, Criminal Procedure Code of Brcko District of Bosnia and Herzegovina).

Traffic data are defined by the term “Telecommunications data” as prescribed in Article 3 Item s) of the Decision of the special obligations of legal and natural persons who provide telecommunications services, administer telecommunications networks and perform telecommunications services, in terms of providing and maintaining capacity that would allow authorized agencies to carry out lawful interception of telecommunications, as well as the capacity for storing and providing telecommunications data, which reads: “*Telecommunications data*”, for the purpose of safeguarding and securing of telecommunications data in accordance with this Decision, are:

- 1) Signaling data contained in or related to the telecommunications for the purpose of any telecommunication system in which it is transmitted;

- 2 ) information on the provision of telecommunications services or systems to any person or on their use by any person, other than the content of any telecommunications except traffic data contained therein, and
- 3) Any other information in the possession of the telecommunication operator which provides or provided services, such as information about the subscriber.

According to the Federal Ministry of the Interior, the data on traffic are considered the data arising between two or more users.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

The conditions to be met are defined in the applicable provisions of the Criminal Procedure Code (quoted in the answer to question 4).

State Investigation and Protection Agency lists the following requirements:

- a. If there is a criminal offense and that in order to illuminate the case and detect the perpetrators they request information;
- b. Monitoring the suspects who are subject to criminal proceedings during their communication with other persons or suspects.

## 4.5 Bulgaria

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

### GAMBLING ACT

In force from 01.07.2012

#### SUPPLEMENTARY PROVISION

§ 1. Within the meaning of this Act:

...

10. "IP address" shall be a unique address which is used for identification of each computer and the devices in the computer network using the Internet.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

### LAW FOR PROTECTION OF THE PERSONAL DATA

Prom. SG. No. 1 of 4 January 2002. amend. SG. No. 70 of 10 August 2004. amend. SG. 93 of 19 October 2004. amend. SG. 43 of 20 May 2005. amend. SG. 103 of 23 December 2005. amend. SG. 30 of 11 April 2006. amend. SG. 91 of 10 November 2006. amend. SG. 57 of 13 July 2007. amend. SG. 42 of 5 June 2009. amend. SG. 94 of 30 November 2010. amend. SG. 97 of 10 December 2010. amend. SG. 39 of 20 May 2011. amend. SG. 81 of 18 October 2011. amend. SG. 105 of 29 December 2011. amend. and supplemented. SG. No. 15 of 15 February 2013.

Art. 2. (Suppl. - SG. 70, 2004, effective 01.01.2005, amended. - SG. 103 of 2005)

(1) (Amended - SG. 91 2006 on) Personal data is any information relating to a natural person who is identified or can be identified, directly or indirectly by an identification number or to one or more specific signs.

According to the statement № 1659/07.04.2011 of the Commission for Protection of personal data "The IP address should be considered as information constituting personal data in all cases in which allows or promotes direct or indirect identification of the user – an individual."

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

### Electronic Communications Act

Art. 248.

(1) (Amended and supplemented. - SG. 105 of 2011 , effective 29.12.2011 ) The enterprises providing public electronic communications networks and/or services, including networks supporting devices for data collection and identification, can process subscriber data when they are directly intended for the providing of electronic communications services.

(2) Subscriber data include:

1. Traffic data - data necessary for the providing of electronic communications services, for charging, for the formation of the bills of subscribers and to prove their authenticity:

a) The number of the calling and the called end-user, card number for online payment;

- b) Start and end of call, specified by date and time to the nearest second, if technically possible, and/or if transfer of data – the volume of transferred data for charging purposes;
  - c) The type of service provided;
  - d) Points of interconnection of the call, the start and end of their use, determined by date and time to the nearest second, if technically possible;
  - e) Details of the type of connection or zones - time and geographical, necessary to determine the value of the service;
  - f) The location of the user of a service, provided by mobile network, including the providing of "roaming";
2. Data necessary for billing and for proving their reliability, including the following data:
- a) Details of subscribers:
    - For individuals - full name, identification number and address, and for foreign entities - personal number;
    - For legal entities and individuals - sole traders - name, location, address and the relevant identification code;
  - b) Type of electronic communications services;
  - c) The total number of units charged for the period for a periodic account;
  - d) The value of the used services for that period;
  - e) Information associated with the selected by the subscriber payment method, and payments made by the subscriber and due by the subscriber;
  - f) Information on changes in the use of the service - restriction of use, cancellation of the restriction;
3. Location data - data that is processed in electronic communication networks for determining the geographic location of the electronic communication equipment of the subscriber.

Art. 250a. (New - SG. 17 of 2010, effective 10.05.2010)

(1) The enterprises providing public electronic communications networks and/or services retain for a period of 12 months data generated or processed in the process of their activities, which is necessary for:

- 1. Trace and identify the source of the link;
- 2. Identifying the destination of the link;
- 3. Identify the date, time and duration of the connection;
- 4. Identifying the type of the connection;
- 5. Identification of electronic communication terminal of a user or of what is presented to his terminal;
- 6. Establish the identifier of the used cells.

(2) Data under par. 1 are stored for the purpose of detection and investigation of serious crimes and crimes under Art. 319a - 319e of the Penal Code, and to search for persons.

(3) Other data, including revealing the content of the messages can be stored in this way.

(4) The enterprises providing public electronic communications networks and/or services are required to destroy data after the deadline under par. 1.

(5) For data that is accessed and have been stored, the head of the authority making the request for access may request the enterprise which has provided them, to maintain them for a period not longer than 6 months from the date of grant.

(6) The data under par. 1 is processed and stored in accordance with the requirements of the protection of personal data.

Art. 251a. (New - SG. 17 of 2009)

(1) (Amended - SG. 17 of 2010, effective 10.05.2010) the data under Art. 250a, para. 1, item 1 are at:

- 1. Public telephone service - telephone number of the caller and the identification data of the subscriber or user;

2. Internet access , internet email and internet telephony - the identifier assigned to the user, identifier of the user and the phone number, assigned to any communication entering the public telephone network, data to identify the subscriber or user to whom the defined IP address, user identifier or telephone number at the time of connection.

(2) (Amended - SG. 17 of 2010, effective 10.05.2010) the data under Art. 250a, para. 1, item 2 are at:

1. Public telephone service - dialed number (called phone number) and in the case of additional services, such as call forwarding or call transfer - the number or numbers to which the call is routed, and the identification data of the subscriber or user;
2. Internet email and internet telephony - user identifier or telephone number of the recipient/s of Internet telephony call, data to identify the subscriber or user and identifier of the recipient for whom the message is intended.

(3) (Amended - SG. 17 of 2010, effective 10.05.2010) the data under Art. 250a, para. 1 item 3 are:

1. The public telephone service - the date and time of beginning and end of the connection;
2. internet access, internet email and internet telephony - date and time of entry and exit to/from the Internet access service, based on a certain time zone, together with the IP address - dynamic or static, assigned for the connection from the service provider, and identifier of the subscriber or user, date and time of entry and exit to/from e-mail service or Internet telephony, based on a certain time zone.

(4) (Amended - SG. 17 of 2010, effective 10.05.2010) the data under Art. 250a, para. 1, item 4 are:

1. Type of the public telephone service;
2. The Internet service for Internet e-mail or internet telephony.

(5) (Amended - SG. 17 of 2010, effective 10.05.2010) the data under Art. 250a, para. 1, 5 are in:

1. fixed telephone service - the calling and the called telephone number;
2. public telephone service provided by mobile terrestrial network - for calling and called telephone number; international identifier of the calling mobile subscriber (IMSI); international identifier of the called mobile subscriber (IMSI); international identifier of the calling mobile electronic communication device (IMEI); international identifier of the calling mobile electronic communication device (IMEI); in case of prepaid services - date and time of the initial activation of the service and the location label - cell ID from which the service is activated and to identify the subscriber or user;
3. internet access , internet email and internet telephony - calling telephone number for dial-up access, digital subscriber line (DSL) or other end point of the originator of the connection.

(6) (Amended - SG. 17 of 2010, effective 10.05.2010) Data on art. 250a, para. 1, item 6 are the administrative addresses of the mobile terrestrial electronic communications network cells, from which is generated or terminated the call.

#### SUPPLEMENTARY PROVISION

§ 1. For the purposes of this Act:

1. "Subscriber" is any natural or legal person who is a party to a contract with an enterprise providing public electronic communications services.

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

## Electronic Communications Act

Art. 250b. (New - SG. 17 of 2010, effective 10.05.2010)

(1) The right to request inspection of the data under Art. 250a, para. 1 according to their competence are the heads of:

1. Specialized directorates, regional directorates and autonomous territorial departments of the State Agency "National Security";
2. General Directorate "National Police", General Directorate "Border Police", Directorate "Internal Security", the Capital Directorate of the Ministry of Interior and the regional directorates of the Ministry of Interior;
3. The "Military Information" and "Military Police" services at the Ministry of Defense;
4. National Intelligence Service.

(2) Access to data under Art. 250a, para. 1 is allowed after a written motivated request from the head of the corresponding bodies under para. 1, comprising:

1. The legal basis and the purpose for which the access is required;
2. Registration number of the file, which requires the access;
3. Data that should be reflected in the report;
4. Period of time;
5. Designated official to whom to provide the data.

(3) For requests made by the bodies under para. 1, a special register should be kept, which is not public.

Art. 250c. (New - SG. 17 of 2010, effective 10.05.2010)

(1) Access to data under Art. 250a, para. 1 is carried out with the authorization of the Chairman of the District Court or authorized by him judge, at the seat of the authority that requested the access, to which shall issue an order granting access to the data.

(2) The order under par. 1 shall contain:

1. Data that should be reflected in the report;
2. Period of time;
3. Designated official to whom to provide the information;
4. Name, title and signature of the judge.

(3) The respective district courts shall keep a special register for the granted or denied orders, which is not public.

(4) For the purposes of criminal proceedings the data under Art. 250a, para. 1 is provided to the court and pre-trial authorities under the terms and conditions of the Criminal Procedure Code.

(5) Access to data under Art. 250a, para. 1, which relates to the Chairman of the District Court, his descendant, sibling, spouse or person, who is in actual marital cohabitation, is carried out with the authorization of the Chairman of the Regional court.

Art. 250d. (New - SG. 17 of 2010, effective 10.05.2010)

(1) The enterprises providing public electronic communications networks and/or services are required to ensure the 24 hours a day, 7 days a week receipt of the order of art. 250c, para. 1 and Art. 251, para. 2.

(2) The heads of enterprises providing electronic communications networks and/or services send to the Commission for Communications Regulation a list indicating:

1. Current address for the order of art. 250c, para. 1 and Art. 251, para. 2;
2. Name, surname and title of authorized officials who receive orders under Art. 250c, para. 1 and Art. 251, para. 2 and their phone numbers; when changing this data, within 24 hours to notify in writing the Commission for Communications Regulation, and its President shall promptly provide the lists of the heads of bodies under art. 250b, para. 1.



Art. 250e. (New - SG. 17 of 2010, effective 10.05.2010)

(1) The enterprises providing public electronic communications networks and/or services, conduct inquiries of the referenced under Art. 250a, para. 1 data, after receiving the order for access. Incoming orders for access are registered in a special register which is not public.

(2) The enterprises providing public electronic communications networks and/or services in the shortest possible time, but not more than 72 hours of receipt of the order for access under art. 250c, para. 1 and Art. 251, para. 2, send the data to the official under Art. 250c, para. 2, item 3. The Minister of the Interior or authorized in writing by him can set a definite time limit within which the data to be sent.

(3) Inquiries for the data under Art. 250a, para. 1 at enterprises providing public electronic communications networks and/or services may be performed only by officials authorized in writing by the respective Head of the enterprise.

(4) After preparing its report signed by the head of the enterprise providing public electronic communications networks and/or services, or authorized in writing by him official. The report shall be registered in a special register and sent to the specified in the order official.

(5) Where available, the order of the judge and report under par. 4 can be sent electronically in compliance with the E-Government Act and the Electronic Document and Electronic Signature Act.

Art. 250f. (New - SG. 17 of 2010, effective 10.05.2010) the report under Art. 250c, para. 4, which is not used in pre-trial proceedings, is destroyed within 6 months from the date of its receipt by three-member committee, comprising nominated by the Head of the bodies under Art. 250b, para. 1, and a record for that shall be created.

Art. 251. (Amended - SG. 17 of 2009, amended. - SG. 17 of 2010, in force from 10.05.2010)

(1) The data under Art. 250a, para. 1 may be provided at the request of a competent authority of another country when this is provided by an international agreement in force for the Republic of Bulgaria.

(2) Access to data under Art. 250a, para. 1 is authorized after request from the Head of a General or Specialized Directorate under Art. 250b, para. 1, item 1 and 2, with permission from the Chairman of the Sofia City Court or authorized by him judge, for which an order issued to provide access to the data. For permits granted or denied the Sofia City Court shall keep a special register which is not public.

(3) For the result from access to data under Art. 250a, para. 1, the competent authority of the requesting State shall be notified as provided by international treaty.

## Criminal Procedure Code

Article 159 Obligation to hand over objects, papers, computerised data, data about subscribers to computer information service and traffic data.

(1) Upon request of the court or the bodies of pre-trial proceedings, all institutions, legal persons, officials and citizens shall be obligated to preserve and hand over all objects, papers, computerized data, including traffic data, that may be of significance to the case.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

See replies to question 4.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

## Electronic Communications Act

Art. 248....

(2) Subscriber data include:

1. Traffic data - data necessary for the providing of electronic communications services, for charging, for the formation of the bills of subscribers and to prove their authenticity, including:

- a) The number of the calling and the called end-user, card number for online payment;
- b) Start and end of call, specified by date and time to the nearest second, if technically possible, and/or if transfer of data – the volume of transferred data for charging purposes;
- c) The type of service provided;
- d) Points of interconnection of the call, the start and end of their use, determined by date and time to the nearest second, if technically possible;
- e) Details of the type of connection or zones - time and geographical, necessary to determine the value of the service;
- f) The location of the user of a service, provided by mobile network, including the providing of "roaming";

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

See replies to question 4.

## 4.6 Croatia

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

–  
Croatian law defines only the term "electronic telecommunications address", which includes IP address along with other types of telecommunications address (telephone etc.).

The Electronic Communications Act (Article 2, paragraph 1, subparagraph 1):

- *address*: the total of all components of addressing (signs, letters, digits and signals) used to determine the destination of a connection.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

Yes, regarding IP address assigned by the ISP to a natural person.

The Act on Personal Data Protection (Article 2, paragraph 1, subparagraph 1):

Personal data means any information relating to an identified natural person or an identifiable natural person (hereinafter: data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

Ordinance on the Manner and Conditions for the Provision of Electronic Communications Networks and Services (Article 8):

- (1) Operator of public communications services shall, in case the application of a natural or legal person for establishment of subscription is accepted, enable access to its public communications network.
- (3) The application form referred to in paragraph 1 of this Article, determined by the operator, shall include in particular:
  - 1. name and seat for legal persons, or name and address for applicants who are natural persons,...
  - 7. connection point address where the subscriber shall be provided with access to public communications network,
  - 8. address for delivery of notifications and address for delivery of bills for provided electronic communications services,
  - 9. e-mail address at which the subscriber wants to receive notification in cases of contracted Internet access services.

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

Criminal Procedure Code:

Article 261

(1) Objects which have to be seized pursuant to the Penal Code or which may be used to determine facts in proceedings shall be temporarily seized and deposited for safekeeping.

(2) Whoever is in possession of such objects shall be bound to surrender them upon the request of the State Attorney, the investigator or the police authorities. The State Attorney, the investigator or the police authorities shall instruct the holder of the object on consequences arising from denial to comply with the request.

Article 263

(1) The provisions of Article 261 of this Act also apply to data saved on the computer and devices connected thereto, as well as on devices used for collecting and transferring of data, data carriers and subscription information that are in possession of the service provider...

(2) Data referred to in paragraph 1 of this Act must be handed over to the State Attorney upon his written request in an integral, original, legible and understandable format. The State Attorney shall stipulate a term for handing over of such data in his request. ...

Article 264

(2) Legal entities may request that data related to their business be not disclosed.

(4) A decision on disclosure of data referred to in paragraph 2 of this Article shall be made by the investigating judge or the court before which the hearing is conducted upon the motion with a statement of reasons of the State Attorney. The ruling of the court before which the hearing is conducted shall not be subject to appellate review.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

There is no procedural difference between obtaining the subscriber information regarding specific person and obtaining the subscriber information regarding specific IP address.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

—  
The Electronic Communications Act (Article 110, paragraph 1):

- data necessary to trace and identify the source of a communication;
- data necessary to identify the destination of a communication;
- data necessary to identify the date, time and duration of a communication;
- data necessary to identify the type of communication;
- data necessary to identify users' communication equipment or what purports to be their equipment;
- data necessary to identify the location of mobile communication equipment.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

Procedure regarding registered owner or registered user:

Criminal Procedure Code (Article 339a, Checking the establishment of telecommunications contacts)

(1) If grounds for suspicion exist that a registered owner or user of telecommunications source has committed a criminal offense subject to public prosecution, the police authority shall, upon the order of the investigative judge and for the purpose of collecting evidence, request the public telecommunications service provider to determine identity, duration and frequency of communication with certain electronic communications addresses, position of a communications device, location of persons establishing electronic communications and identification marks of device.

(2) The police authority may, upon the order of the investigative judge, request the public telecommunications service provider checking referred to in paragraph 1 of this Article for the registered owner or user of telecommunications source connected with a person suspected of having committed a criminal offense subject to public prosecution.

(3) The decision on the request of the public prosecutor investigating judge shall issue within four hours. The investigative judge shall issue the order referred to in paragraph 1 and 2 of this Article upon the written motion with a statement of reasons of the State attorney.

(4) By way of exception, if there is a risk of delay and the State attorney has reason to believe that he will not be able to obtain an order of a judge, an order referred to in paragraph 1 and 2 of this Article may be issued by the competent State attorney.

(5) The order referred to in paragraph 4 of this Article and the letter which will explain the reasons for its issuance the State attorney shall promptly, but not later than 24 hours after issuance, submit to the investigating judge.

(6) The investigating judge shall decide on the legality of the order of the State attorney within 48 hours from the receipt of letter. The State attorney can not file an appeal against the ruling of the investigating judge.

...

(8) The order to check the establishment of telecommunications contacts is not required if the registered owner or user of communications source has given written consent.

Procedure regarding unregistered owner or unregistered user (prepaid mobile Internet service, public hotspot etc.):

Law on Police Activities and Powers (Article 68, Checking the establishment of telecommunications contact)

(1) In order to prevent danger and violence, prevent and detect criminal offenses subject to public prosecution, a police officer may request the telecommunications service provider to check the identity, duration and frequency of contact between certain telecommunications addresses.

(2) The checking referred to in paragraph 1 of this Article may include determination of location where have been persons establishing telecommunications contact and identification marks of device.

(3) The checking referred to in paragraph 1 of this Article shall be conducted upon the written approval of the head of a crime investigation division within the Ministry of Interior or a person authorized by him.

## 4.7 Czech Republic

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

Yes, it is defined in the regulation num. 357/2012 on archiving, passing on and disposal of traffic data:

For the purpose of this regulation an "IP address" is understood as an identifier used in internet protocols to unambiguous determination of the end point and is unique during the time of the communication.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

Yes, it is considered to be personal data as soon as it is connected to a specific subject of data. Art. 4 letter a) of Act num. 101/2000 Coll. on Protection of Personal Data:

Personal data is for the scope of this Act understood to be any information relating to a specified or specifiable subject of data. A subject of data is considered specified or specifiable if it can be directly or indirectly identified especially on the basis of number, code, one or more elements specific to his physical, physiological, psychical, cultural, social or economic identity.

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

The counterpart of Convention's term 'subscriber information' is Czech legal system's 'personal data', which is understood very widely as any information relating to a specified or a specifiable subject of data. The full definition is cited above.

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

Information relevant for criminal proceedings is acquired on the basis of Art. 78 of the Criminal Proceedings Code:

Those who are carrying a thing important to the criminal proceedings are obligated to submit it to the court, public prosecutor, or police authority when prompted; if the purpose of the criminal proceedings requires its securing, they are obligated to release the property when prompted. When prompted, it is necessary to note that if they fail to comply with the call, the property may be removed from them, as well as there being other consequences of non-compliance (Section 66).

Furthermore, in case telecommunication information is sought, the Criminal Proceedings Code states the following conditions (Section 88a):

- An intentional crime with the upper limit of severity of sentence of at least three years is being prosecuted or one of several explicitly mentioned crimes is being prosecuted or a crime which the Czech Republic is obliged to prosecute by an international treaty is being prosecuted.

- The aim followed (by acquiring the information) cannot be reached otherwise, or it would be severely more difficult to reach otherwise.
- Order issued by a head judge or by a judge on the proposal of a prosecutor.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

A police body must request their supervising prosecutor to propose the matter to a judge. If the judge issues the order, anyone having the information is obliged to hand it over.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

Article 2 of the regulation num. 357/2012 on archiving, passing on and disposal of operating and localizing data:

Extent of the archiving of operating and localizing data

(1) In the public telephone networks with circuit switching the following operating and localizing data (herein after referred to as „data“) shall be archived:

- a) Phone numbers of the calling and called person, phone number taking part in the conference call, identifier of the phone card used in the public telephone booth
- b) Date and time of the initiation of communication,
- c) Duration of communication,
- d) Date and time of text message SMS sending,
- e) Used telephone service in accordance with article 1 letter m),
- f) State of communication,
- g) Supplementary data according to paragraph 4, if any data according to the letter a) or paragraph 5 is missing;

(2) In the public mobile networks all data stated in paragraph 1 with an exception of the identifier of the phone card shall be archived. Furthermore these data shall be archived:

- a) IMSI identifier of the calling and called person,
- b) Identifier of the mobile device of the calling and called person,
- c) Date and time of the multimedia message MMS sending,
- d) Indication of the base station Start and the base station Stop,
- e) Supplementary data stated in paragraph 4, if any data according to the paragraph 1 letter a), except for the phone card identifier, or paragraph 5 is missing.

(3) In the electronic communication with packet switching the data shall be archived as follows:

- a) In the service of access to the internet via the fixed internet connection
  1. Type of the connection,
  2. Phone number or identification of user,
  3. Identifier of the user's account,
  4. MAC address of the device of the user's service,
  5. Date and time of initiating and terminating internet connection,
  6. Indication of the access point of the wireless internet connection,
  7. IP address and port number that were used for internet connection;

b) In the service of the mobile access to internet connection

1. Type of the connection,
2. Phone number of the user,
3. Identifier of mobile device,
4. Date and time of initiating and terminating of internet connection,
5. Indication of the base station Start and the base station Stop
6. IP address and port number that were used for internet connection;

c) In the service of the access to the electronic mail box

1. IP address and port number that were used for internet connection,
2. Identifier of the user's account,
3. Date and time of initiating connection to the electronic mail box,
4. Date and time of terminating of the connection to the electronic mail box,
5. Identifier of the protocol of the electronic mail box;

d) In the service of the transfer of the electronic mail messages

1. IP address and port number of the message source and target,
2. Date and time of sending of the message,
3. Address of the sender's electronic mail,
4. Addresses of the receiver's electronic mails,
5. State of the transfer of the message,
6. Identifier of the protocol of the electronic mail;

e) In the service of the IP telephony

1. IP address and port number of the source device,
2. IP address and port number of the target device,
3. Transmission Protocol,
4. Date and time of the initiation and termination of communication
5. Supplementary data stated in paragraph 4, if data identifying the called and calling person or any data stated in paragraph 5 is missing;

f) In the service of the internet access according to letter a) or b) with translation of IP addresses

1. Private IP address,
2. Public IP address and port number or assigned scale of ports,
3. Date and time of the address translation initiation,
4. Date and time of the address translation termination.

(4) Supplementary data in the paragraph 1 letter g), paragraph 2 letter e) and paragraph 3 letter e) point 5 are

- a) Destination or country code of international incoming calls' origin,
- b) Code of the operator of interconnected public communication network or provider of public accessible telephone network provided via interconnection,
- c) Name of legal person, name alternatively names and surname of natural person in business arranging non-public communication network and its identification number.

(5) In the networks stated in paragraphs 1-3 name alternatively names and surname, participant's address or registered user's address stated in the contract or location address of the telecommunication end device shall be archived.

(6) Furthermore these data shall be archived:



- a) Data on all public telephone booths stating their phone numbers, registration numbers, geographic coordinates in the World Geodetic System 1984 (WGS84)(herein after referred to as „Coordinate system WGS 84“) and verbal description of location,
- b) Data on all base stations stating their indication alternatively all other used identifiers, geographic coordinates in the Coordinate system WGS 84, azimuth of antennas routing and verbal description of location,
- c) Data on mutual connections between phone numbers and IMSI identifiers and mobile device identifiers,
- d) In prepaid services date and time of the activation of service and indication of the base stations within reach when activation was done,
- e) Data on all access points with their indication stated, alternatively all other used identifiers, furthermore geographic coordinates in the Coordinate system WGS 84, azimuth of antennas routing and verbal description of location.

(7)Data on time shall be archived in local time, in accordance with this regulation. In case local time does not correspond to the time in the Czech Republic, data on time shall be given with the indication of the time zone.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

The procedure is the same as described in answer to question number 5.

## 4.8 Denmark

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

No, the term "IP-address" is not defined specifically for criminal law purposes in Danish legislation.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

Depending on the circumstances, IP addresses may be considered as personal data under the Act on Processing of Personal Data.

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

There is no generally applicable definition of subscriber information in Danish legislation.

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

Section 13 of Consolidation Act No. 128 of 7 February 2014 on electronic communications networks and services prescribes that providers of electronic communications networks and services for end users shall, at the request of the police, hand over information identifying the access of an end user to electronic services. This would include subscriber information. Section 13 applies, inter alia, to subscriber information for static IP addresses.

In so far as dynamic IP addresses are concerned, the obtainment of subscriber information requires the imposition of an order on the Service Provider to hand over information in the possession of someone who is not a suspect to the police, pursuant to section 804, paragraph 1 of the Administration of Justice Act. Such order may be imposed if there is reason to assume that the information may serve as evidence in a criminal case.

The order shall be imposed by a court, unless for reasons of urgency the police deem it impossible to await the decision of the court, in which case the police may administratively impose the order. The police shall bring the administratively imposed order before the courts as soon as possible and within 24 hours, if the Service Provider so requests, pursuant to section 806, paragraph 4 of the Administration of Justice Act.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

See above under question 4.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

There is no generally applicable definition of traffic data in Danish legislation.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

According to Danish legislation, interferences with the confidentiality of communications, including traffic data, by the police or judicial authorities generally require a court decision authorising the interference in question.

The court may only authorise the interference, if it is satisfied that there are concrete reasons for presuming that the means of communication in question is used to deliver messages to or from a suspect, and that the interference is presumed to be of vital importance to an investigation concerning a serious crime, pursuant to section 781 of the Administration of Justice Act.

The interference shall be imposed by a court, unless for reasons of urgency the police deem it impossible to await the decision of the court, in which case the police may administratively impose the interference. The police shall bring the administratively imposed interference before the courts as soon as possible and within 24 hours, pursuant to section 783, paragraph 4 of the Administration of Justice Act.

## 4.9 Estonia

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

No. The term „IP-address is not defined.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

Yes, an IP-address is considered to be as personal data.

Personal Data Protection Act

Article 4 Personal Data

(1) Personal data are any data concerning an identified or identifiable natural person, regardless of the form or format in which such data exist.

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

According to the Article 2 15) of the Electronic Communications Act the subscriber means a person using publicly available electronic communications services who has a contract with a communications undertaking for the use of the publicly available electronic communications services.

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

Police or other investigating body can request the subscriber information within a criminal proceeding related to any criminal offence. The principle of *ultima ratio* has to be respected.

Criminal Procedure Code

§ 90<sup>1</sup>. Request to electronic communications undertakings to submit information

(1) A body conducting proceedings may make enquiries to electronic communications undertakings about the data required for the identification of an end-user related to the identification tokens used in the public electronic communications network, except for the data relating to the fact of transmission of messages.

(2) With the permission of a Prosecutor's Office an investigative body may make enquiries in pre-trial procedure or with the permission of a court in court proceeding to electronic communications undertakings about the data listed in subsections 111<sup>1</sup> (2) and (3) of the Electronic Communications Act and not specified in the first subsection of this section. The permission to make inquiries shall set out the dates of the period of time about which the requesting of data is permitted.

(3) The enquiries prescribed in this section may be made only if this is unavoidably necessary for the achievement of the objectives of criminal proceedings.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

Same as the previous reply.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

- Traffic data is considered to be data provided by the Article 111<sup>1</sup> (2)(3) of the Electronic Communications Act except the information on subscriber.
  
- Electronic Communications Act  
§ 111<sup>1</sup>. Obligation to preserve data  
(2) The providers of telephone or mobile telephone services and telephone network and mobile telephone network services are required to preserve the following data:
  - 1) the number of the caller and the subscriber's name and address;
  - 2) the number of the recipient and the subscriber's name and address;
  - 3) in the cases involving supplementary services, including call forwarding or call transfer, the number dialled and the subscriber's name and address;
  - 4) the date and time of the beginning and end of the call;
  - 5) the telephone or mobile telephone service used;
  - 6) the international mobile subscriber identity (*IMSI*) of the caller and the recipient;
  - 7) the international mobile equipment identity (*IMEI*) of the caller and the recipient;
  - 8) the cell ID at the time of setting up the call;
  - 9) the data identifying the geographic location of the cell by reference to its cell ID during the period for which data are preserved;
  - 10) in the case of anonymous pre-paid mobile telephone services, the date and time of initial activation of the service and the cell ID from which the service was activated.

(3) The providers of Internet access, electronic mail and Internet telephony services are required to preserve the following data:

  - 1) the user IDs allocated by the communications undertaking;
  - 2) the user ID and telephone number of any incoming communication in the telephone or mobile telephone network;
  - 3) the name and address of the subscriber to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;
  - 4) the user ID or telephone number of the intended recipient of an Internet telephony call;
  - 5) the name, address and user ID of the subscriber who is the intended recipient in the case of electronic mail and Internet telephony services;
  - 6) the date and time of beginning and end of the Internet session, based on a given time zone, together with the IP address allocated to the user by the Internet service provider and the user ID;
  - 7) the date and time of the log-in and log-off of the electronic mail service or Internet telephony service, based on a given time zone;
  - 8) the Internet service used in the case of electronic mail and Internet telephony services;
  - 9) the number of the caller in the case of dial-up Internet access;
  - 10) the digital subscriber line (*DSL*) or other end point of the originator of the communication.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

Criminal Procedure Code

§ 90<sup>1</sup>. Request to electronic communications undertakings to submit information

(1) A body conducting proceedings may make enquiries to electronic communications undertakings about the data required for the identification of an end-user related to the

identification tokens used in the public electronic communications network, except for the data relating to the fact of transmission of messages.

(2) With the permission of a Prosecutor's Office an investigative body may make enquiries in pre-trial procedure or with the permission of a court in court proceeding to electronic communications undertakings about the data listed in subsections 111<sup>1</sup> (2) and (3) of the Electronic Communications Act and not specified in the first subsection of this section. The permission to make inquiries shall set out the dates of the period of time about which the requesting of data is permitted.

(3) The enquiries prescribed in this section may be made only if this is unavoidably necessary for the achievement of the objectives of criminal proceedings.

## 4.10 Finland

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

Traffic data monitoring is regulated in Chapter 10 of Coercive measures act (806/2011). Section 6 regulates telecommunications monitoring (not interception which is different issue), e.g. obtaining of identification information regarding a message which has been sent from a teleaddress. According to said provision "Traffic data monitoring refers to the obtaining of identifying data regarding a message that has been sent from or received by a network address or terminal end device connected to a telecommunications network referred to in section 3, the obtaining of location data regarding the network address or the terminal end device, or the temporary prevention of the use of the network address or terminal end device. Identifying data refers to data referred to in section 2, paragraph 8 of the Act on the Protection of Privacy in Electronic Communications (516/2004) that can be connected to the subscriber or user and that is processed in telecommunications networks in order to transmit or distribute messages or keep messages available.

According to provision of act 516/2004 referred to above "*identification data* means data which can be associated with a subscriber or user and which is processed in communications networks for the purposes of transmitting, distributing or providing messages". For these purposes IP address is considered to be identification information.

Term "IP address" itself is not expressly more precisely defined.

(unofficial and non-up to date translations of acts 806/2011 and 516/2004 are attached to e-mail which will be sent together with this questionnaire).

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

According to personal data act (523/1999) section 3 subsection 1 "*personal data* means any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household." In these circumstances referred to above IP address may be personal data.

Finland is also bound by the EU directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Its definitions in the article 2 are therefore relevant.

(unofficial and non-up to date translations of act 523/1999 is attached to e-mail which will be sent together with this questionnaire).

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

These categories are not expressly and exhaustively listed. However section 36 subsection 2 of the "old" police act (493/1995) is clarifying. According to it the police have the right to obtain from a telecommunications operator and a corporate or association subscriber the contact information about a subscription that is not listed in a public directory or the data specifying a telecommunications subscriber connection, an e-mail address or other telecommunications address, or telecommunications terminal equipment if, in individual cases, the information is needed to carry out police duties.

Similarly, the police have the right to obtain postal address information from organisations engaged in postal services.

According to subsection 4 "Separate provisions apply to telecommunications interception, telecommunications monitoring and gathering information on the location of mobile stations". In other words, this provision refers to coercive measures act referred to in question 1.

New police act (872/2011, entry into force 1.1.2014) is not yet available in English. However, its main content regarding the question what information is covered, is the same.

To sum up: IP address of a subscriber might be subscriber information in the sense mentioned in police act. However, in cases referred to in Coercive measures act it can be traffic data.

(Unofficial and non-up-to-date translation of the old police act 493/1995 is attached to e-mail which will be sent together with this questionnaire).

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

In cases referred to police act it is enough "if, in individual cases, the information is needed to carry out police duties". In situations falling under coercive measures act and traffic data monitoring different rules apply. See Chapter 10 (section 6) of the attached coercive measures act.

Subscriber information can be obtained by the police also based on Criminal Investigation Act (805/2011) Chapter 7 section 8 regarding the obligation of a witness to provide evidence. Subsection 1 and 2 of the said provision read as follows:

" (1) A witness shall truthfully and without concealment state what he or she knows in the matter under investigation. However, if he or she would have the right or the obligation in the criminal proceedings concerning the matter to refuse to testify, reveal a circumstance or answer a question, he or she has said right or obligation also in the criminal investigation.

(2) A witness who has the obligation to provide evidence referred to in subsection 1 is also obliged to produce a document or other evidence in his or her possession that has significance from the point of view of the criminal investigation."

(Unofficial and non-up to date translations of act 805/2011 is attached to e-mail which will be sent together with this questionnaire.)

Powers and procedures of Act on the Exercise of Freedom of Expression in Mass Media (460/2003) are presented under question 5.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

See answer to questions 1, 3 and 4. Regarding traffic data monitoring see Coercive measures act, Chapter 10, especially sections 6 – 9.

In addition to this, in cases of expression of opinions in mass media, the powers and procedures referred to in Act on the Exercise of Freedom of Expression in



Mass Media (460/2003) are relevant (unfortunately no up to date translation available. Unofficial and non-up-to-date translation of the act 460/2003 is attached to e-mail which will be sent together with this questionnaire).

According to section 17 of the said act, on the request of an official with the power of arrest, as referred to in chapter 2, section 9(1), of the Coercive Measures Act (806/2011), a public prosecutor, or an injured party, a court may order the keeper of a transmitter, server or other similar device to release the information required for the identification of the sender of a network message to the requester, provided that there are probable reasons to believe that the contents of the message are such that providing it to the public is a criminal offence. However, the identifying information may be ordered to be released to the injured party only in the event that he or she has the right to bring a private prosecution for the offence. The request shall be filed with the District Court of the domicile of the keeper of the device, or with the District Court of Helsinki, within three months of the publication of the message in question. The court may reinforce the order by imposing a threat of a fine.

A court order on the release of identifying information shall be open to appeal as a separate matter. The order shall not be enforced until it has become final, unless the appellate court otherwise orders.

Identifying information may be ordered to be released on the request of the authorities of a foreign state, if the provision of the relevant message to the public would constitute an offence in Finland under the prevailing circumstances, or if the release is based on an international agreement or on some other international obligation binding on Finland.

The term "network message" is defined in section 2(2) of said act.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

–

See answer to question 1 above.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

See answer to question 1 and Chapter 10 (section 6) of the attached coercive measures act (attached). Some traffic data can also be obtained in the context of data preservation order referred to in Chapter 8 section 24 subsection 3 of the Coercive measures Act (see attached) in order to identify service providers.

Section 24 read as follows:

Data retention (preservation) order:

(1) If, before the search of data contained in a device, there is reason to assume that data that may be of significance for the clarification of the offence is deleted or is changed, an official with the power of arrest may issue a data retention order. Such an order requires that a person holding or administering data, not however the suspect in an offence, maintains the data unchanged. The order may apply also to data that can be assumed to be transmitted to a device or information system within the month following the issuing of the order. On request a written certificate shall be given of the order, detailing the data that is the object of the order.

(2) What is provided in subsection 1 applies also to data in a message transmitted by an information system that relates to the origin, destination, routing and size of the message as well as to the time,

duration, nature and other corresponding factors of the transmission (transmission information). (1146/2013)

(3) A criminal investigation authority does not, on the basis of the retention order referred to in subsection 1, have the right to obtain information on the contents of the message, transmission information or other recorded information. If several service providers have participated in the transmission of the message referred to in subsection 2, a criminal investigation authority has the right to obtain the transmission information necessary to identify the service providers. (1146/2013)

## 4.11 France

**Question 1 : La notion "d'adresse IP" est-elle définie aux fins de droit pénal dans votre législation nationale (lois pénales, règlementaires ou techniques ou règlement) Si oui, veuillez indiquer le texte de loi ou le règlement.**

Il n'existe pas de texte dans la législation nationale française définissant explicitement l'adresse IP.

**Question 2 : L'adresse IP est-elle considérée comme étant une donnée personnelle? Si oui, veuillez indiquer le texte correspondant.**

Pas de définition claire en France, et pas de jurisprudence complètement établie à ce sujet ; La Commission Nationale Informatique et Libertés chargée de veiller au respect des libertés individuelles dans le cadre de l'utilisation de l'informatique, estime que l'adresse IP est une donnée personnelle, au sens **de l'article 2, alinéa 2 de la loi informatique et Libertés du 6 janvier 1978**, à savoir : »Constitue une donnée à caractère personnel, toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres « .

Pour autant, la Cour d'Appel de Paris a estimé en avril 2007 que l'adresse IP ne constituait pas un traitement de données au sens du droit de l'informatique et des libertés.

Un arrêt de la Cour de Cassation le 13/01/2009 a jugé qu'il ne s'agissait pas d'une donnée identifiable et donc ne constituait pas une donnée à caractère personnel telle que définie par la législation française.

**Question 4 : Quelles catégories de données sont considérées comme des données relatives aux abonnés? Veuillez indiquer le texte.**

La définition la plus complète est fournie par le chapitre II de l'article 6 de la loi 2204/575 du 21 juin 2004, loi pour la confiance dans l'économie numérique, et précisées par le décret 2011-219 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu en ligne.

Il s'agit de :

- nom, prénom, raison sociale,
- adresses postales associées,
- pseudonymes utilisés,
- adresses de courrier électronique ou de comptes associées,
- numéros de téléphone,
- mot de passe ainsi que les données permettant de le vérifier ou de le modifier,
- type de paiement utilisé,
- référence du paiement,
- montant,
- date et heure de la transaction.

Il s'agit également des identifiants de connexion à l'origine de la communication, du type de protocoles utilisés pour la connexion au serveur, et pour le transfert des contenus, de la nature de l'opération, des dates et heures, ainsi que de l'identifiant fourni par l'auteur de l'opération lorsque celui ci l'a fourni.

**Question 4 : Dans le cadre d'une enquête pénale, quelles exigences doivent être remplies afin de permettre à la police ou à l'autorité judiciaire d'obtenir les données relatives aux abonnés auprès d'un fournisseur de service?**

Toute demande de la part des autorités judiciaires doit faire l'objet d'une réquisition judiciaire établie par un officier de police judiciaire dûment habilité et mentionnant le cadre légal d'enquête ainsi que les infractions visées. Aucune information concernant les données relatives aux abonnés, comme au trafic, ne peut être obtenue en dehors du cadre légal.

**Question 5 : Plus précisément, quelles conditions doivent être remplies afin de permettre à la police ou à l'autorité judiciaire d'obtenir les données relative aux abonnés pour une adresse IP spécifique, dans le cadre d'une enquête pénale ?**

Idem.

**Question 6 : Quelles catégories de données sont considérées comme des données de trafic dans votre législation nationale ? Veuillez indiquer le texte.**

—  
Les données de trafic sont définies en France comme étant des données techniques liées à l'utilisation des réseaux qu'il s'agisse de communications téléphoniques, de courriers électroniques, d'accès à un site internet, de SMS, ou de services de messagerie multimédia (MMS) et permettent d'identifier les interlocuteurs, leur localisation et la durée de leur communication. Elles sont évoquées dans l'article **L34-1 du Code des Postes et des Communications Electroniques, introduit par l'article 20 de la loi 2003-239 du 18 mars 2003 sur la sécurité intérieure ;**

Cet article instaure les dérogations au principe général d'effacement des données et encadre les modalités de conservation de ces données de trafic.

—

**Question 7 : Dans le cadre d'une enquête pénale, quelles exigences doivent être remplies pour permettre à la police ou à l'autorité judiciaire d'obtenir des données de trafic auprès d'un fournisseur de service?**

Idem qu'au numéro 4.

## 4.12 Germany

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

The term "IP address" has not been given a statutory definition.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

The Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG) defines personal data as follows:

Section 3 of the Federal Data Protection Act

(1) "Personal data" shall mean any information concerning the personal or material circumstances of an identified or identifiable natural person ("data subject").

Static IP addresses are personal data (connection identifiers) in the sense of section 3 (1) of the Federal Data Protection Act.

As a general rule, however, end customers will use dynamic IP addresses to access the internet. These are not permanently allocated to a specific person (a specific connection). Where the dynamic IP address and the appurtenant time are known, it is possible to use these traffic data to determine the customer data of the allocation holder to whom the connection is assigned at that specific point in time. Accordingly, if the allocation holder can be identified using the IP address, then the (dynamic) IP address is a personal datum pursuant to section 3 (1) of the Federal Data Protection Act.

The provision concerning the creation of a link between a dynamic IP address and the customer data of the allocation holder is set out in subsection 2 of section 100j of the Code of Criminal Procedure (*Strafprozessordnung*, StPO):

Section 100j of the Code of Criminal Procedure

(1) Insofar as necessary to establish the facts or determine the whereabouts of an accused person, information on data collected pursuant to sections 95 and 111 of the Telecommunications Act may be requested from any person providing, or collaborating in the provision of, telecommunications services on a commercial basis (section 113 (1), sentence 1, of the Telecommunications Act). If the request for information pursuant to sentence 1 refers to data by means of which access to terminal equipment, or to storage media installed in such terminal equipment or physically separate therefrom, is protected (section 113 (1), sentence 2, of the Telecommunications Act), information may only be requested if the statutory requirements for the use of such data have been met.

(2) The information pursuant to subsection (1) may also be requested by reference to an Internet Protocol address assigned to a specific time (section 113 (1), sentence 3, of the Telecommunications Act).

...

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

The term "customer data", which encompasses said subscriber information, has been defined in section 3 no. 3 of the Telecommunications Act (*Telekommunikationsgesetz*, TKG) as follows:

"Customer data" means the data of a subscriber collected for the purpose of establishing, framing the contents of, modifying, or terminating a contract for telecommunications services;

Customer data may be stored by the service provider in the context of the contractual relationship pursuant to section 95 of the Telecommunications Act:

Section 95 of the Telecommunications Act

(1) The service provider may collect and use customer data to the extent required for achieving the purpose referred to in section 3 no. 3. Under a contractual relationship with another service provider, the service provider may collect and use the customer data of his subscribers and of the subscribers of the other service provider to the extent required for performance of the contract between the service providers. Transmission of the customer data to third parties, unless permitted by this Part or by another law, shall be carried out only with the subscriber's consent.

(2) The service provider may use the customer data of the subscribers referred to in subsection (1), sentence 2, for subscriber advisory purposes, for promoting his own offerings, for market research, and in order to inform about an individual wish of another user to enter into a dialogue only to the extent required for such purposes and provided the subscriber has given his consent. A service provider who, under an existing customer relationship, has lawfully received notice of a subscriber's telephone number or postal address, including his electronic address, may use these for the transmission of text or picture messages to a telephone or postal address for the purposes referred to in sentence 1, unless the subscriber has objected to such use. Use of the telephone number or address according to sentence 2 shall be permitted only if the subscriber, when the telephone number or address is collected or first stored and on each occasion a message is sent to such telephone number or address for one of the purposes referred to in sentence 1, is given information in clearly visible and easily readable form that he may object at any time, in writing or electronically, to the dispatch of further messages.

(3) When the contractual relationship ends, the customer data are to be erased by the service provider upon expiry of the calendar year following the year in which the contract terminated. Section 35 (3) of the Federal Data Protection Act applies accordingly.

(4) In connection with the establishment of, or modification to, a contractual relationship or with the provision of telecommunications services, the service provider may require presentation of an official identity card where this is necessary to verify the subscriber's particulars. The service provider may make a copy of the identity card. The copy is to be destroyed by the service provider without undue delay once the particulars of the subscriber needed for the conclusion of the contract have been established. The service provider may not use data other than the data permitted under subsection (1).

(5) The provision of telecommunications services may not be made dependent upon the subscriber's consent to use of his data for other purposes where the subscriber is not able, or is not able in reasonable manner, to access such telecommunications services in another way. Any consent granted under such circumstances shall be invalid.

Additionally, data are to be stored for requests for information filed by security authorities pursuant to section 111 of the Telecommunications Act, also insofar as these are not required for operational purposes:

Section 111 of the Telecommunications Act

(1) Any person commercially providing, or assisting in providing, telecommunications services and in so doing assigning telephone numbers or other allocation identifiers, or providing telecommunications connections for telephone numbers or other allocation identifiers assigned by other parties is, for the information procedures according to sections 112 and 113, to collect, prior to activation, and store without undue delay

1. the telephone numbers and other allocation identifiers,
2. the name and address of the allocation holder,
3. the date of birth in the case of natural persons,
4. in the case of fixed lines, additionally the address for the line,
5. in cases, in which a mobile terminal device is made available in addition to a mobile telephony connection, the device number of said device, as well as
6. the effective date of the contract

even if such data are not required for operational purposes; where known, the date of termination of the contract is likewise to be stored. Sentence 1 also applies where the data are not included in directories of subscribers (section 104). The obligation to immediately store the data stipulated in sentence 1 applies accordingly regarding those data set out in sentence 1 nos. 1 and 2 for any person providing, on a commercial basis, a publicly accessible electronic mail service and, in this context, collecting data pursuant to sentence 1 nos. 1 and 2, in which context the "data" referred to in sentence 1 no. 1 will be replaced by the "identifiers of the electronic mailboxes" and the "allocation holder" referred to in sentence 1 no. 2 will be replaced by the "holder of the electronic mailbox." A person with obligations according to sentence 1 or sentence 3 receiving notice of any changes is to correct the data without undue delay; in this connection the person with obligations according to sentence 1 is subsequently to collect and store data not yet recorded if collecting the data is possible at no special effort. The manner in which data for the information procedure according to section 113 are stored is optional.

(2) Where the service provider according to subsection (1) sentence 1 or sentence 3 operates in conjunction with a sales partner, such partner shall collect data according to subsection (1) sentences 1 and 3 under the pre-requisites set out therein and shall transmit to the service provider, without undue delay, these and data collected under section 95; subsection (1) sentence 2 applies accordingly. Sentence 1 also applies to data relating to changes, inasmuch as the sales partner receives notice of them in the course of normal business transactions.

(3) Data within the meaning of subsection (1) sentence 1 or sentence 3 need not be collected subsequently for contractual relationships existing on the date of entry into force of this provision, save in the cases referred to in subsection (1) sentence 4.

(4) The data are to be erased upon expiry of the calendar year following the year in which the contractual relationship ended.

(5) No remuneration is granted for the collection or storage of data.

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

Access to customer data has been provided for at two levels. On the one hand, section 113 of the Telecommunications Act defines the customer data that service providers are fundamentally allowed to make available. The conditions and pre-requisites under which this may be done have been provided for in the laws governing the activities of the requesting law enforcement and judicial authorities.

The service providers may provide customer data to law enforcement and police authorities pursuant to section 113 of the Telecommunications Act as follows:

Section 113 of the Telecommunications Act

(1) In accordance with subsection (2), any person commercially providing or assisting in providing telecommunications services may use the data collected pursuant to sections 95 and 111 in accordance with the provisions of the present stipulation in order to comply with his obligations to provide information to the authorities listed in subsection 3. This also applies to data by means of which access to terminal equipment, or to storage media installed in such terminal equipment or

physically separate therefrom, is protected. The data to be included in such information may also be determined by means of an IP address allocated to a specific point in time; for this purpose, traffic data may also be evaluated using automated processing. The entirety of all internal data sources are to be used in providing information pursuant to sentence 3.

(2) The information may be provided only inasmuch as an authority listed in subsection 3 has requested, in text form, that this be done in an individual case for purposes of prosecuting crimes or administrative offences, to avert dangers to public safety or the public order, or to perform the statutory tasks of the authorities listed in subsection 3 no. 3; such request must include a reference to a provision of the law allowing such authority to collect the data referenced in subsection (1); no data obtained pursuant to subsection (1) may be transmitted to other public or non-public authorities. In exigent circumstances, the information may be provided also in those cases in which the request was made in other than text form. In such event, a subsequent confirmation of the request is to be issued immediately in text form. The authorities listed in subsection 3 are responsible for ensuring the permissibility of the request for information.

(3) Authorities in the sense of subsection 1 are

1. The authorities responsible for prosecuting crimes or administrative offences;
2. The authorities responsible for averting dangers to public safety or the public order;
3. The authorities serving the protection of the constitution at the level of the Federation and of the *Länder*, the Military Counterintelligence Service (*Militärischer Abschirmdienst*, MAD), and the Federal Intelligence Service (*Bundesnachrichtendienst*, BND).

(4) Any person commercially providing or assisting in providing telecommunications services is to transmit the data that are to be provided immediately and completely. The parties obligated are to keep the request for information and the provision of information confidential vis-à-vis the data subjects and vis-à-vis third parties.

(5) Any person commercially providing or assisting in providing telecommunications services is to make the arrangements required in his sphere of responsibility for the provision of information and shall do so at his costs. Any such person who serves more than 100,000 customers is to keep available, for the receipt of the requests for information and for the issuance of the appurtenant information, a secured electronic interface in accordance with the Technical Directive provided for by section 110 (3), which interface is to warrant that the transmission is also protected against unauthorised parties becoming aware of the data. In this context, it is to be ensured that each request for information is reviewed by a responsible technical specialist as to its complying with the formal requirements set out in subsection (2), and that it is released for further processing only after such review has obtained a positive result.

The access by law enforcement authorities to such data has been provided for in section 100j of the Code of Criminal Procedure:

Section 100j of the Code of Criminal Procedure

(1) Insofar as necessary to establish the facts or determine the whereabouts of an accused person, information on data collected pursuant to sections 95 and 111 of the Telecommunications Act may be requested from any person providing or collaborating in the provision of telecommunications services on a commercial basis (section 113 (1), sentence 1, of the Telecommunications Act). If the request for information pursuant to sentence 1 refers to data by means of which access to terminal equipment, or to storage media installed in such terminal equipment or physically separate therefrom, is protected (section 113 (1), sentence 2, of the Telecommunications Act), information may only be requested if the statutory requirements for the use of such data have been met.

(2) The information pursuant to subsection (1) may also be requested by reference to an Internet Protocol address allocated to a specific time (section 113 (1), sentence 3, of the Telecommunications Act).



(3) Requests for information pursuant to subsection (1), sentence 2, may be ordered by the court only upon application by the public prosecution office. In exigent circumstances the order may also be issued by the public prosecution office or by its investigative personnel (section 152 of the Courts Constitution Act). In this case a court decision is to be sought without delay. The first to third sentences shall not apply if the data subject already has or must have knowledge of the request for information or if the use of the data has already been permitted by a court decision. The fulfilment of the conditions pursuant to the fourth sentence shall be documented.

(4) In the cases referred to in subsection (1), sentence 2, and subsection (2), the data subject shall be notified of the request for and provision of information. Notification shall take place insofar as and as soon as this can be effected without thwarting the purpose of the information. It shall be dispensed with where overriding interests meriting protection of third parties or of the data subject himself constitute an obstacle thereto. Where notification is deferred pursuant to sentence 2 or dispensed with pursuant to sentence 3, the reasons therefor shall be documented.

(5) On the basis of a request for information pursuant to subsections (1) or (2), any person commercially providing or assisting in providing telecommunications services shall transmit without delay the data required for the provision of the information. Section 95 subsection (2) shall apply *mutatis mutandis*.

Comparable provisions regarding access to data have been set out in the Act governing the Activities of the Federal Criminal Police Office (*Bundeskriminalamtsgesetz*, BKAG) (section 7, section 20b, section 22), the Act on the Federal Police (*Bundespolizeigesetz*, BPolG) (section 22a), the Customs Investigation Service Act (*Zollfahndungsdienstgesetz*, ZFdG) (section 7, section 15), the Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution (*Bundesverfassungsschutzgesetz*, BVerfSchG) (section 8d), the Act concerning the Federal Intelligence Service (*Gesetz über den Bundesnachrichtendienst*, BNDG) (section 2b), the Act on the Activities of the Military Counterintelligence Service (*MAD-Gesetz*, MADG) (section 4b) and in the laws governing the activities of the requesting authorities of the federal *Länder*.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

Pursuant to section 100j (2) of the Code of Criminal Procedure, the pre-requisites concerning the request for and provision of information that apply for IP addresses generally are the same as those concerning other customer data (see question 4).

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

The term "traffic data" has been defined in section 3 no. 30 of the Telecommunications Act as "data collected, processed or used in the provision of a telecommunications service." Section 96 of the Telecommunications Act has defined the traffic data that may permissibly be stored by service providers:

Section 96 of the Telecommunications Act

(1) The service provider may collect and use the following traffic data to the extent required for the purposes set out in this Chapter–

1. the number or other identification of the lines in question or of the terminal, personal authorisation codes, additionally the card number when customer cards are used, additionally the location data when mobile handsets are used;
2. the beginning and end of the connection, indicated by date and time and, where relevant to the charges, the volume of data transmitted;
3. the telecommunications service used by the user;
4. the termination points of fixed connections, the beginning and end of their use, indicated by date and time and, where relevant to the charges, the volume of data transmitted;
5. any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes.

Such traffic data may be used only inasmuch as this is necessary for the purposes set out in sentence 1 hereof or purposes established by other stipulations of the law, or in order to set up further connections. Otherwise, traffic data are to be erased by the service provider without undue delay following termination of the connection.

(2) Any collection or use of traffic data extending above and beyond the provisions made in subsection (1) is impermissible.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

The requirements that must be met in order to obtain information on traffic data have been set out in the laws governing the activities of the requesting authorities. For the law enforcement authorities, they have been provided for in section 100 g of the Code of Criminal Procedure as follows:

Section 100g of the Code of Criminal Procedure

(1) If certain facts give rise to the suspicion that a person, either as perpetrator or accessory,

1. has committed a criminal offence of substantial significance in the individual case as well, particularly one of the offences referred to in Section 100a (2), or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence, or
2. has committed a criminal offence by means of telecommunication,

then, to the extent that this is necessary to establish the facts or determine the accused's whereabouts, telecommunications traffic data (section 96 (1), section 113a of the Telecommunications Act) may be obtained also without the knowledge of the data subject. In the case referred to in sentence 1, number 2, the measure shall be admissible only where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success and if the acquisition of the data is proportionate to the importance of the case. The acquisition of location data in real time shall be admissible only in the case of sentence 1, number 1.

(2) Section 100a (3) and section 100b subsections (1) to (4), sentence 1, shall apply *mutatis mutandis*. In derogation from section 100b (2), sentence 2, number 2, in the case of a criminal offence of substantial significance, a sufficiently precise spatial and temporal description of the telecommunication shall suffice where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success or be much more difficult.

## 4.13 Japan

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

The term "IP address" is not defined for criminal law purposes in our domestic legislation.

The definition of "IP address" for non-criminal law purposes is given under Art. 24.5.14 of the "Regulations for Enforcement of the Telecommunications Business Law" as "numbers assigned to identify telecommunication equipment used to communicate via internet protocol".

(Note: English translation for the "Regulations for Enforcement of the Telecommunications Business Law" is not available.)

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

We are not in a position to be able to formally respond to this question as Japan is not a Party to the "Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", which is referred to in the preamble of the Convention on Cybercrime, and we probably do not share the definition of "personal data" under this question.

On the other hand, in our domestic law, the "Act on the Protection of Personal Information" defines "personal information" as "information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual)." In light of this definition, IP address with which ISP can easily identify a specific individual by matching it with time stamps etc., may be considered as personal information under this Act. The Ministry of Internal Affairs and Communications developed in August 2004 the "Guideline on Protection of Personal Information in Telecommunications Business" in order to provide concrete guidelines for telecommunication carriers concerning appropriate handling of personal information and manages its operation.

The Act on the Protection of Personal Information  
Article 2

(1) The term "personal information" as used in this Act shall mean information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual).

(Note: English translation for the "Guideline on Protection of Personal Information in Telecommunications Business" is not available.)

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

There are no provisions concerning the so-called "subscriber information" under our domestic law. In general, information such as subscriber's name, physical address, contact information, date of contract, unique IP address statically assigned to the subscriber concerned may be considered as "subscriber information."

Please note however that, pursuant to Art. 21(2) of the Constitution of Japan which guarantees secrecy of communication, Art. 4(1) of the Telecommunications Business Act protects secrecy of communications handled by telecommunications carrier. "Secrecy of communication" is considered to include, not only the content of individual communication, but also time, date and place of individual communication, as well as identification codes of the party(/ies) to the individual communication, such as one's name, address, domicile and telephone number.

The Constitution of Japan

Art. 21

[...]

(2) No censorship shall be maintained, nor shall the secrecy of any means of communication be violated.

The Telecommunications Business Act

Article 4 (Protection of Secrecy)

(1) The secrecy of communications being handled by a telecommunications carrier shall not be violated.

[...]

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

In general, "subscriber information" may be provided by ISP upon request from investigation authority as a report concerning necessary matters related to the investigation pursuant to Art. 197(2) of the Code of Criminal Procedure. (However, if the information is considered to fall under "secrecy of communication" described in our response to Q3, investigation authority usually needs seizure warrant issued by a judge to obtain such information.)

Code of Criminal Procedure

Article 197

(1) With regard to investigation, such examination as is necessary to achieve its objective may be conducted; provided, however, that compulsory dispositions shall not be applied unless special provisions have been established in this Code.

(2) Public offices or public or private organizations may be asked to make a report on necessary matters relating to the investigation.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

In general, when the IP address concerned is statically assigned to a unique subscriber (i.e. in the case of static IP address), the information as to whom the concerned IP address is assigned to may be provided by ISP upon request from investigation authority as a report concerning necessary matters related to the investigation pursuant to Art. 197(2) of the Code of Criminal Procedure.

However, IP address related to specific communication is typically considered to be protected as "secrecy of communication". Hence, if the investigation authority requests information as to whom the concerned IP address is assigned to by linking the static IP address concerned to a specific

communication, in general, the information concerning the subscriber is also considered to enjoy protection as "secrecy of communication", thus requiring seizure warrant issued by a judge.

Similarly, when the IP address concerned is not statically assigned to a unique subscriber (i.e. in the case of dynamic IP address), such IP address is also considered to be related to specific communication. Hence, if the investigation authority requests information as to whom the concerned IP address is assigned to, in general, the information concerning the subscriber is also considered to enjoy protection as "secrecy of communication", thus requiring seizure warrant issued by a judge.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

Under our domestic law, there is no definition of "traffic data." However, according to Art. 197(3) of the Code of Criminal Procedure, at least the origin, the destination, date and time of telecommunication would be considered as "traffic data".

(Note: Art. 197(3) of the Code of Criminal Procedure is a new provision concerning request for preservation of traffic data. English translation provided below is an unofficial translation. Please do not quote in any official documents.)

Code of Criminal Procedure

Article 197

(3) [Unofficial translation] A public prosecutor, a public prosecutor's assistant officer or a judicial police official may, when it is necessary for seizure or seizure with a record order, request in writing, a person who engages in the business of providing electronic communication facility for communications of others or a person whose facility for his own electronic communications is capable of transmitting electronic communications among unspecified or many persons to preserve necessary part of the electromagnetic records, which are recorded in the course of business, by specifying the origin, destination, time and other traffic data of the electronic communication for a period not exceeding 30 days. In this case, when it is deemed that the necessity of seizure or seizure with a record order of the electromagnetic records does no longer exist, a public prosecutor, a public prosecutor's assistant officer or a judicial police official shall rescind the request.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

In our domestic law, the so-called "traffic data" as described in Q6 is considered to be protected as "secrecy of communication" (please refer to our response to Q3). In principle, when telecommunication carriers including ISP provide information concerning secrecy of communication to investigation authority, they need to do so in accordance with the warrant issued by a judge. Therefore, in order for investigation authority to obtain "traffic data" from ISP, in general, seizure warrant issued by a judge is required.

#### 4.14 Latvia

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

The term "IP address" isn't clearly defined by domestic legislation of the Republic of Latvia.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

Under the domestic legislation of the Republic of Latvia IP address isn't being clearly defined as personal data, unlike other data which may be attached to it (such as name of the subject, username or address).

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

Specific categories of data are not defined by domestic legislation of the Republic of Latvia.

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

Under the section 71 of the Electronic Communication Law of the Republic of Latvia, information which is being used to identify user or subscriber may be submitted for the pre-trial investigation. Following the court decision, other information may be submitted to the law enforcement authorities. Submitted information may contain traffic data of the user/subscriber in question. Such data may be submitted only in case if it has been recognized by the court as acceptable, based on the rights of user/subscriber and its protection. Information may not be submitted in case if technical capabilities of ISP are not sufficient to generate, process and register required information.

According to the Criminal Procedure Law of the Republic of Latvia part 2, section 10, article 192, when the criminal procedure has been started, the judge may request the ISP to hand over saved traffic data (as covered by part 2, section 10, article 191 of the Criminal Procedure Law) according to the procedure defined by Electronic Communication Law.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

According to the section 71 of the Electronic Communication Law of the Republic of Latvia, information may be submitted to the pre-trial investigation services, national security agencies, and public prosecution office or to the court, following the formal request of mentioned bodies. The process of information collection and submission is being defined by the Cabinet.

According to the Criminal Procedure Law of the Republic of Latvia part 2, section 10, article 192, when the criminal procedure has been started, the judge may request the ISP to hand over saved traffic data (as covered by part 2, section 10, article 191 of the Criminal Procedure Law) according to the procedure defined by Electronic Communication Law.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

According to the section 1.1(29)of the Electronic Communication Law of the Republic of Latvia, any information or data, which is being processed in order to transmit information via electronic communication network or generate bills and calculate payments, except for the actual content of transmitted information.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

Police or judicial authority can obtain traffic data from a Service Provider by making a request.

#### 4.15 Lithuania

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

The "IP address" is included in the legal definition of the term "number of terminal equipment" provided for in the Paragraph 4 of the Description of the General Conditions for Pursuit of Electronic Communication Activities, approved by the Order No. 1V-340, 8 April, 2005 of the Director of the Communications Regulatory Authority of the Republic of Lithuania (Official Gazette, 2005, No. 49 1641): "**Number of terminal equipment** – digit sequence or its symbolic equivalent (including telephone number, international mobile equipment identifier (IMEI), international mobile subscriber identifier (IMSI), Internet Protocol (IP) number, e-mail address) that identifies the terminal equipment or network termination point at which the terminal is connected so that the data can be routed to the appropriate terminal equipment or network termination point", therefore it is not defined in the domestic legislation of the Lithuania as the separate term.

The broader term "**Electronic communications network identifier** means the addressing facilities identifying electronic communications network points, including network termination points, or terminal equipment connected to an electronic communications network in order to direct information specifically to these electronic communications network points or the relevant terminal equipment or to identify the sender of information" (Article 3 Paragraph 18 of the Law on the Electronic Communications of the Republic of Lithuania, No. IX-2135, 15 April 2004, Official Gazette, No. 69-2382, 2004 (as last amended on 19 December 2013, No XI-XII-712, Official Gazette, No. 140-7078, 2013), hereinafter referred to as "the LEC").

In the context of these legal provisions the "**Terminal equipment** means equipment, or relevant component thereof, capable of receiving and/or sending information and intended to be connected directly or indirectly by any means whatsoever to public communications networks" (Article 3 Paragraph 22 of the LEC).

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

It is provided for in Article 2 Paragraph 1 of the Law on Legal Protection of Personal Data of the Republic of Lithuania, No. I-1374, 11 June 1996 (as last amended on 12 May 2011, No XI-1372) that "**Personal data** shall mean any information relating to a natural person (data subject) who is known or who can be identified directly or indirectly by reference to such data as a personal identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". According to the provision mentioned, an IP address is presumed to be personal data, when relating to a natural person (data subject) who is known or who can be identified directly or indirectly by reference to the IP address (e.g. by reference to the static IP address, which is assigned to a specific person under the contract on the provision of electronic communications services).

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

The term "subscriber information" is not defined in the Lithuanian domestic legislation and no specific data are attributed to it. It is provided for in Article 3 Paragraph 1 of the Law on Electronic Communications that "**Subscriber** means any person who or which is party to a contract with the provider of publicly available electronic communication services for the supply of such services".



According to this legal definition it is presumed that all information available on the basis of the contract on the provision of electronic communication services is "subscriber information" (i. e. the same information, as it is provided for in Article 18 Paragraph 3 of the Cybercrime Convention).

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

Legal requirements to obtain subscriber information from a Service Provider by the police or judicial authority within a criminal investigation are provided for in the Code of Criminal Procedure of the Republic of Lithuania (as last amended by the Law No. XII-777, 13 March, 2014) (hereinafter – CPC of RL).

Subscriber information can be legally obtained by the police or judicial authority within a criminal investigation in the main ways as follows:

1. When an official request (production order) is presented (sent) to any natural or legal person (including service providers), who possesses such an information (Art. 97 of the CPC of RL).
2. When a suspect, an accused person, a legal representative, an advocate, a victim, a civil plaintiff, a civil defendant or their representatives, as well as any natural or legal person provides information (documents or tangible objects) on their own initiative (Art. 98 the CPC of RL). If such an information (document or tangible object) is provided when an investigation action is performed (e. g. during interview of a witness or a suspect), it should be added to the records of this action ("the record" is the procedural document confirming, in the manner laid down by the CPC of RL, the fact that a pre-trial investigation and judicial proceedings have been conducted, their contents and the results).
3. When a decision of a prosecutor is passed and approval of a pre-trial investigation judge is acquired to visit any state or municipal, public or private institution, enterprise, or organisation and request to be allowed to get familiarized with the necessary documents or other information, make records or copies of the documents and information, or acquire information in written if this is necessary for investigation of a criminal offence (Art. 155 Par. 1 of the CPC of RL). Pursuant to Art. 163 of the CPC of RL a fine can be imposed upon persons refusing to provide information or documents requested by the prosecutor (Art. 155 Par. 2 of the CPC).
4. When any actions of criminal investigation are applied by a pre-trial investigator or a prosecutor, the procedural rules relevant to that actions should be followed (e. g. provisional measures – search and seizure).

Upon reasonable belief that there are, in some premises or any other place, instruments of an criminal offence, tangible objects obtained or acquired in a criminal way also objects or documents that might be relevant for the investigation, a pre-trial investigation officer or a prosecutor may carry out search with a view of discovering and seizing them (Art. 145 Par. 1 of the CPC of RL).

If it is necessary to seize tangible objects or documents of value for the investigation, and if is known where and at whose place precisely they are, the pre-trial investigation officer or the prosecutor may effect a seizure.

Search and seizure can be effected only if a reasoned order of the pre-trial judge is adopted and in the presence of the relevant persons only (i.e. owner, tenant, manager of the flat, house or other premises where the search is being conducted, a member or their family or a close relative, and where a search is being carried out an enterprise of an office – in the presence of a representative of that enterprise or office; where there is no possibility to ensure the presence of the above persons, a search shall be carried out in the presence of any other two persons or a representative of a municipal institution) (Art. 145 Par. 3, 4, Art. 147 Par. 1, 3 of the CPC of RL).

The relevant Articles of the CPC of RL:

„Article 97. Order to submit tangible objects and documents relevant to the investigation of a criminal offence or to the trial

A pre-trial investigation officer, a prosecutor and the court has the right to order natural and legal persons to submit tangible objects and documents relevant to the investigation of criminal offences or to the trial.

Article 98. Submission of tangible objects and documents relevant to the investigation of the criminal offence or to the trial

A suspect, an accused, a legal representative, an advocate, a victim, a civil plaintiff, a civil defendant and their representatives, as well as any natural or legal person may, on its own initiative to submit tangible objects and documents relevant to the investigation of the criminal offence or to the trial.

...

Article 147. Seizure

*1. When it is necessary to obtain items or documents important for investigation of a criminal act and location or possessor thereof is known a pre-trial investigation officer or prosecutor may implement seizure. Seizure is imposed by a grounded ruling of a pre-trial investigation judge. In cases of emergency seizure can be implemented by a decision of a pre-trial investigation officer or prosecutor however, in such a case approval of a pre-trial investigation judge in respect of the implemented seizure shall be acquired within three days from the day of actual seizure. Upon failure to acquire approval of a pre-trial investigation judge within said term all the seized items and documents shall be returned to the persons from whom they were seized and the results of the seizure may not be used as evidence of guilt of the suspect or accused person.*

*2. Persons possessing items or documents to be seized shall not obstruct the officers implementing the seizure. Persons failing to comply with his duty may be fined further to the article 163 of this Code.*

*3. During seizure the persons specified in the part 4 article 145 of this Code shall be present.*

*4. If persons possessing the items or documents that must be seized fail to surrender them, the items or documents may be seized with the use of force.*

...

Article 155. Right of a Prosecutor to Get Familiarised with the Information

1. Having passed a decision and acquired approval of a pre-trial investigation judge a prosecutor has the right to visit any national or municipal, public or private institution, enterprise, or organisation and request to be allowed to get familiarized with the necessary documents or other information, make records or copies of the documents and information, or acquire information in written if this is necessary for investigation of a criminal act.

2. Pursuant to article 163 of this Code a fine can be imposed upon persons refusing to provide information or documents requested by the prosecutor.

3. A prosecutor may use the information acquired in the procedure specified in part 1 of this article only for the purpose of investigation of the criminal act. A prosecutor shall immediately destroy information not necessary for investigation of the criminal act.
4. A pre-trial investigation officer can be commissioned by a prosecutor to get familiarized with the information in the procedure defined by this article.
5. Laws of the Republic of Lithuania can establish limitations on the right of a prosecutor to get familiarized with information."

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

Please refer to the answers of the Question 4.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

Legal definition of traffic data is provided for in Article 3 Paragraph 57 of the Law on Electronic Communications: "**Traffic data**" means any data processed for the purpose of the conveyance of a communication on an electronic communications network and/or for the billing thereof". No categories of data are specified as traffic data under the domestic law.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

Please refer to the answers of the Question 4.

#### 4.16 Mauritius

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

IP Address is NOT defined in any of the following: Computer Misuse and CyberCrime Act 2003, Data Protection ACT 2001, Information and Communication Technologies Act 2001.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

As per section 2 of the Data Protection Act

"personal data" means—

data which relate to an individual who can be identified from those data; or

data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion; }

—

To the extent that an individual who can be identified from the IP address, in all likelihood it may be considered to be personal data. However, we do not have local jurisprudence on the issue, but the tendency is to stand guided by the ECJ decisions, given that our legislation (Data Protection Act) was substantially inspired from the EC directive.

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

As per Part 1, Section 2, clause "Subscriber Information" of the Computer Misuse and CyberCrime Act 2003, the following categories of data are considered to be subscriber information:

- a. The type of the communication service used, the technical provisions taken to use the communication service and the period of service
- b. The subscriber's identity, postal or geographical address, telephone and other access number, billing, and payment information, available on the basis of service agreement or arrangement; or
- c. Any other information on the site of installation of communication equipment available on the basis of a service agreement or arrangement.

Comments:

Text:

- a. "subscriber information" means any information, contained in the form of computer data or any other form, that is held by a service provider, relating to subscribers, other than traffic or other data, by which can be established -
- b. the type of the communication service used, the technical provisions taken to use the communication service and the period of the service;
- c. the subscriber's identity, postal or geographical address, telephone and other access number, billing and payment information, available on the basis of a service agreement or arrangement; or
- d. any other information on the site of installation of a communication equipment available on the basis of a service agreement or arrangement;

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

Submission of a **Judge's Order** which authorizes the Service Provider to provide the necessary information.

Requirements:

11. Preservation order

- (1) Any investigatory authority may apply to the Judge in Chambers for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.
- (2) For the purposes of subsection (1), data includes traffic data and subscriber information.
- (3) An order made under subsection (1) shall remain in force -
  - (a) until such time as may reasonably be required for the investigation of an offence;
  - (b) where prosecution is instituted, until the final determination of the case; or
  - (c) until such time as the Judge in Chambers deems fit.

12. Disclosure of preserved data

The investigatory authority may, for the purposes of a criminal investigation or the prosecution of an offence, apply to the Judge in Chambers for an order for the disclosure of-

- (a) all preserved data, irrespective of whether one or more service providers were involved in the transmission of such data;
- (b) sufficient data to identify the service providers and the path through which the data was transmitted; or
- (c) electronic key enabling access to or the interpretation of data.

13. Production order

(1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, an investigatory authority may apply to the Judge in Chambers for an order compelling -

- (a) any person to submit specified data in that person's possession or control, which is stored in a computer system; and
- (b) any service provider offering its services to submit subscriber information in relation to such services in that service provider's possession or control.

(2) Where any material to which an investigation relates consists of data stored in a computer, disc, cassette, or on microfilm, or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

14. Powers of access, search and seizure for the purposes of investigation

(1) Where an investigatory authority has reasonable grounds to believe that stored data would be relevant for the purposes of an investigation or the prosecution of an offence, it may

apply to a Judge in Chambers for the issue of a warrant to enter any premises to access, search and seize such data.

- (2) In the execution of a warrant under subsection (1), the powers of the investigatory authority shall include the power to -
  - (a) seize or secure a computer system or any information and communication technologies medium;
  - (b) make and retain a copy of such data or information;
  - (c) maintain the integrity of the relevant stored data or information; or
  - (d) render inaccessible or remove the stored data or information from the computer system, or any information and communication technologies medium.

#### 15. Real time collection of traffic data

Where the investigatory authority has reasonable grounds to believe that any data would be relevant for the purposes of investigation and prosecution of an offence under this Act, it may apply to the Judge in Chambers for an order -

- (1) allowing the collection or recording of traffic data, in real time, associated with specified communications transmitted by means of any computer system; or
- (2) compelling a service provider, within its technical capabilities, to -
  - (a) effect such collection and recording referred to in subsection (1); or
  - (b) assist the investigatory authority, to effect such collection and recording.

#### 16. Deletion order

A Judge in Chambers may, upon application by an investigatory authority, and being satisfied that a computer system or any other information and communication technologies medium contains indecent photograph of children, order that such data be -

- (1) no longer stored on and made available through the computer system or any other medium; or
- (2) deleted or destroyed.

#### 17. Limited use of disclosed data and information

- (1) No data obtained under sections 11 to 15 shall be used for any purpose other than that for which the data was originally sought except -
  - (a) in accordance with any other enactment;
  - (b) in compliance with an order of a court or Judge;
  - (c) where such data is required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, assessing or collecting tax, duty or other monies owed or payable to the Government;
  - (d) for the prevention of injury or other damage to the health of a person or serious loss of or damage to property; or
  - (e) in the public interest.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

Submission of a Judge's Order which authorizes the SP to provide the necessary information.

Re: above: section 12 and 13; Disclosure of preserved data and Production order

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

As per Part 1, Section 2, "telecommunication network..." Clause (d) of the Data Protection Act 2001, "traffic data" means any data relating to a communication by means of a computer system and generated by the system that form part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying services.

Texts:

Section 2: computer misuse and cybercrime act :

"traffic data" means any data relating to a communication by means of a computer system and generated by the system that form part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Section 2: Data Protection Act:

"traffic data" means any data relating to a communication by means of a computer system and generated by the system that form part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service;

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

Submission of a Judge's Order which authorizes the SP to provide the necessary information.

Re above section 15:

Real Time Collection of traffic Data

15: Real time collection of traffic data

Where the investigatory authority has reasonable grounds to believe that any data would be relevant for the purposes of investigation and prosecution of an offence under this Act, it may apply to the Judge in Chambers for an order –

- (1) allowing the collection or recording of traffic data, in real time, associated with specified communications transmitted by means of any computer system; or
- (2) compelling a service provider, within its technical capabilities, to - effect such collection and recording referred to in subsection (1); or assist the investigatory authority, to effect such collection and recording

Data Protection Act:

13. Preservation Order

(1) The Commissioner may apply to a Judge in Chambers for an order for the expeditious preservation of data, including traffic data, where he has reasonable grounds to believe that such data is vulnerable to loss or modification.

(2) Where the Judge in Chambers is satisfied that an order may be made under subsection (1), he shall issue a Preservation Order specifying a period which shall not be more than 90 days during which the order shall remain in force.

(3) The Judge in Chambers may, on application made by the Commissioner, extend the period specified in subsection (2) for such time as the Judge thinks fit.

(S. 13 not in operation.)

#### 4.17 Moldova

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

The "IP address" is not defined as a term.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

The IP address is not considered personal data. There is not a specific interpretation for it. However in certain circumstances may be considered to be personal data in view of their definition given by Law no. 133 of 08.07.2011 on the protection of personal data, in art. 3 (personal data - any information relating to an identified or identifiable natural person (the subject of personal data). Identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social)

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

–  
User data - any information, data, or as any other form, owned by a service provider, relating to subscribers of such services other than traffic or content data and for determining: the type of service communication used, the technical provisions taken in this regard and the period of service, identity, postal or geographic address, telephone number of the subscriber and any other contact number as well as billing and payment data available under a contract or service arrangement, any other information on where to find communication equipment, available under a contract or arrangement for services, and any other data that may lead to the identification of the user; (Article 2 of Law no. 20 of 03.02.2009 preventing and combating cybercrime)

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

If there does not exist a serious, very serious or extremely serious case apply the article 301 of the Criminal Procedure Code. Criminal actions with the authorization of the investigating judge:

- (1) Authorizing judge shall perform criminal actions related to limiting the inviolability of the person, address, limitation of secrecy of correspondence, telephone conversations, telegraph and other communications and other actions required by law.

If there exists a serious, very serious or extremely serious case apply the article 132/1 of the Criminal Procedure Code: special investigative measures are ordered and carried out if the following conditions are met:

- 1) there is no other way to achieve criminal proceedings or be injured considerably the management of evidence;
- 2) there is a reasonable suspicion about the preparation or commission of a serious, very serious or extremely serious case, with the exceptions established by law;
- 3) the action is necessary and proportionate restriction of human rights and fundamental freedoms.



-

The special investigative measures:

- 2 ) the authorization order of the prosecutor:
- a) identify the subscriber, the owner or operator of an electronic communications system or of an access point to a computer system; Article 132/2 par. (1) Section 2 ) a) of the Criminal Procedure Code.

Article 134/5 of the Code of Criminal Procedure. Identify the subscriber, the owner or operator of an electronic communications system or of an access point to a computer system:

- (1) Identify the subscriber the owner or operator of an electronic communications system or of an access point to a computer system is to request an electronic service provider to identify the subscriber, the owner or user of a telecommunications system , a telecommunications mean or of an access point to a computer system or communicate whether a particular means of communication or access point to a computer system or asset is used or was used or was active at a given time.
- (2) Order of disposition of special investigative measure , in addition to the items referred to in art . 255, will include:
  - 1) the identification of the service provider that has the data specified in par. (1) or keep them under control;
  - 2) identification of the subscriber, the owner or user, if they are known, motivating conditions for the disposal of special investigative measure;
  - 3) the statement of the obligation of the person or service provider to communicate immediately, confidentially the requested information.
- (3) Service providers are obliged to cooperate with the prosecution for the enforcement of the order of the prosecutor and put them immediately to the requested information.
- (4) Persons who are called upon to cooperate with the prosecution are obliged to keep secret operation performed. Breach of this obligation is punishable under the Penal Code.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

-

Not exist specifically requirements because not exist subscriber information for a specific IP address to a specific criminal investigation.

Apply the general rule described in the question four.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

-

Traffic data - any data related to a communication having passed through a computer system, the system produced as part of the communication chain, the origin, destination, route, time, date, size, duration or type of service underlying;

(Article 2 of Law no. 20 of 03.02.2009 on prevention and combating cybercrime)

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

The first situation ( if you are currently a serious, very serious or extremely serious case)

Article 132/1 of the Criminal Procedure Code: special investigative measures are ordered and carried out if the following conditions are met:

- 1) there is no other way to achieve criminal proceedings or be injured considerably the management of evidence;
- 2) there is a reasonable suspicion about the preparation or commission of a serious, very serious or extremely serious , with the exceptions established by law;
- 3) the action is necessary and proportionate to restriction of human rights and fundamental freedoms.

Article 132 /2 par. (1) point 1 ) h) of the Criminal Procedure Code: to the discovery and investigation of criminal offenses shall include the special investigative measures:

- 1 ) authorizing judge:
- h) collection of information by electronic communication service providers;

Article 134<sup>4</sup> . Collecting information from providers of electronic communications

- Collecting information from providers of electronic communications and computer data traffic consists of collecting institutions telecommunications, from fixed or mobile operators, the operators of Internet technical information sent by telecommunications channels (telegraph, fax , paging , computer , radio and other channels), securing secret information transmitted or received through technical lines telecommunication links by persons subject to special investigative measure and operators to obtain information held about users of telecommunications services including roaming about their telecommunications services, which are assigned:
  - 1) the owners of phone numbers;
  - 2) telephone numbers registered in the name of a person;
  - 3) user telecommunications services;
  - 4) the source of communication (telephone number of the caller , name, surname and address of the subscriber or registered user );
  - 5) destination communication ( telephone number or called party number to which the call was routed, redirected , name, surname , address of the subscriber or user);
  - 6) the type, date, time and duration of communication , including unsuccessful call attempts;
  - 7) user communications equipment or other device used for communication ( mobile phone IMEI , Cell ID location name );
  - 8) the whereabouts of the mobile device at the beginning of communication , geographical location of the cell.

The second situation (if you are not currently a serious, very serious or extremely serious case)  
Article 301 of the Criminal Procedure Code. Criminal prosecution with the authorization of the investigating judge:

- The judge authorizing prosecution is carried out actions related to limit the inviolability of the person, address, limit secrecy of correspondence, telephone conversations, telegraph and other communications and other actions required by law.



## 4.18 Montenegro

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

Term "IP address" is not defined in Montenegrin criminal law. Only definition that we have is from Law on electronic communication, which defined "address":

Definitions

Article 4

Some of the terms used in this law shall have the following meaning:

1) Address is a series or combination of decimal digits, symbols and additional information used to identify particular terminal points of a connection to public electronic communications network;

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

Montenegrin Law on personal data don't recognize IP address as personal data.

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

Law on electronic communications prescribe definition of subscriber as "Subscriber is any natural person or legal entity who or which is a party to a contract with an operator of publicly available electronic communications services for the supply of such services"

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

Police or judicial authority can obtain subscriber information when they have condition that there are elements of the criminal offense. There is no need for concrete name of subscriber and formal criminal investigation, only condition is that there is suspicion of criminal offense.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

Police or judicial authority can obtain subscriber information for specific IP address when they have condition that there are elements of the criminal offense. There is no need for concrete name of subscriber and formal criminal investigation, only condition is that there is suspicion of criminal offense.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

Law on electronic communications define traffic data as: "the data processed for the purpose of provision of electronic communications services or for the purpose of the calculation and billing thereof".

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

Only condition is that there are elements of the criminal offense.

## 4.19 Norway

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

The term "IP address" is not used, but several laws refer to IP addresses as "electronic communication addresses".

One example: The Electronic Communications Act of June 14, 2003, Section 2-9:

Providers and installers have a duty to maintain secrecy on the content of electronic communications and others' use of electronic communications, including information on technical systems and methods. (...)

The duty of confidentiality does not prevent information being given to the prosecuting authority of the police on contract-based telephone numbers or other subscription information, as well as **electronic communications addresses**. The same applies in giving evidence in court. Nor does the duty of confidentiality prevent information as mentioned in the first paragraph being given to another authority pursuant to the law.

A request from the prosecuting authority or the police for information as described in the third paragraph shall be complied with unless special circumstances make this inadvisable.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

An IP address can be considered to be personal data, according to the Norwegian Data Protection Act. The Personal Data Act ("Personopplysningsloven") is based on the European Data Protection Directive (95/46/EC). Section 2 in the Data Protection Act is similar to Article 2 in the Directive.

The Norwegian Data Protection Act, Section 2 Definitions:

### Section 2 Definitions

For the purposes of this Act, the following definitions shall apply:

- 1) personal data: any information and assessments that may be linked to a natural person,
- 2) processing of personal data: any use of personal data, such as collection, recording, alignment, storage and disclosure or a combination of such uses,
- 3) personal data filing system: filing systems, records, etc. where personal data is systematically stored so that information concerning a natural person may be retrieved.
- 4) controller: the person who determines the purpose of the processing of personal data and which means are to be used,
- 5) processor: the person who processes personal data on behalf of the controller,
- 6) data subject: the person to whom personal data may be linked,
- 7) consent: any freely given, specific and informed declaration by the data subject to the effect that he or she agrees to the processing of personal data relating to him or her,
- 8) sensitive personal data: information relating to
  - a) racial or ethnic origin, or political opinions, philosophical or religious beliefs,

- b) the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act,
- c) health,
- d) sex life,
- e) trade-union membership.

Based on this general definition, the Norwegian Data Protection Authority considers IP addresses to be indirectly identifiable personal data, for example in a case where a Norwegian law firm representing MPA and IFPI wanted to collect and store IP addresses connected to illegal file sharing of copyrighted material.

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

There is a partial definition regarding subscriber information in the Electronic Communications Act of June 14, 2003, Section 2-9:

Providers and installers have a duty to maintain secrecy on the content of electronic communications and others' use of electronic communications, including information on technical systems and methods. (...)

The duty of confidentiality does not prevent information being given to the prosecuting authority of the police on **contract-based telephone numbers or other subscription information**, as well as electronic communications addresses. The same applies in giving evidence in court. Nor does the duty of confidentiality prevent information as mentioned in the first paragraph being given to another authority pursuant to the law.

A request from the prosecuting authority or the police for information as described in the third paragraph shall be complied with unless special circumstances make this inadvisable.

As a part of new regulations regarding the upcoming implementation of the Data Retention Directive, the Electronic Communications Act was amended with a new Section 2-7a, first subsection:

Provider of electronic communication networks used for public electronic communication service and others who offer such service, have a duty to store traffic data, positioning data and data necessary to identify the subscriber or user in 6 months, for use in investigation and prosecution of serious criminal offences. This duty relates to data generated or treated in the providers electronic communication network by use of fixed-line phone, mobile phone, Internet telephony, Internet access and e-mail.

This duty is described in further detail in the Data Retention Regulation ("Datalagrings-forskriften") Chapter 2. This regulation is currently not implemented, but is scheduled to be implemented by July 1, 2015.

(A copy of this regulation is enclosed to this questionnaire, in case more details should be of interest.)

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

Based on the Electronic Communication Act Section 2-9. Third subsection, basic subscriber data can be obtained from a Service Provider, without a court order:

Providers and installers have a duty to maintain secrecy on the content of electronic communications and others' use of electronic communications, including information on technical systems and methods. (...)

The duty of confidentiality does not prevent information being given to the prosecuting authority of the police on contract-based telephone numbers or other subscription information, as well as electronic communications addresses. The same applies in giving evidence in court. Nor does the duty of confidentiality prevent information as mentioned in the first paragraph being given to another authority pursuant to the law.

A request from the prosecuting authority or the police for information as described in the third paragraph shall be complied with unless special circumstances make this inadvisable.

The Electronic Communication Act regulates Service Providers, such as phone companies and ISPs, based on the definitions in Chapter 1. Services like website hosting, social media providers, domain registrars etc, are not regulated by this law. For subscriber/customer data from these services, the general rules in the Criminal Procedure Act apply (production order etc).

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

According to the Electronic Communication Act, Section 2-9:

Providers and installers have a duty to maintain secrecy on the content of electronic communications and others' use of electronic communications, including information on technical systems and methods. (...)

The duty of confidentiality does not prevent information being given to the prosecuting authority of the police on contract-based telephone numbers or other subscription information, as well as electronic communications addresses. The same applies in giving evidence in court. Nor does the duty of confidentiality prevent information as mentioned in the first paragraph being given to another authority pursuant to the law.

A request from the prosecuting authority or the police for information as described in the third paragraph shall be complied with unless special circumstances make this inadvisable.

The Criminal Procedure Act Section 170a describes the general principle for use of of coercive measures:

A coercive measure may be only used when there is sufficient reason to do so. The coercive measure may not be used when it would be a disproportionate intervention in view of the nature of the case and other circumstances.

Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.

There is not specific definition of "traffic data" as such, but The Electronic Communication Act, the Data Retention Regulation, the Criminal Procedure Act as well as case law describes what is considered "traffic data" (and not subscriber data or positioning data).



**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

Traffic data is considered more sensitive than customer data.

To obtain historical traffic data, the Norwegian Post and Telecommunications Authority must release the Service Provider in question from the duty of secrecy, according to the Criminal Procedure Act Section . 118, first subsection.

(According to annual statistics from the Post and Telecom Authority, about 1 in 10 requests from the prosecutors for historical traffic data, are not accepted.)

This is done case by case. After this, the prosecution must get a production order issued by the local district court. In cases of urgency, a production order may be issued by the prosecutor, but this must be brought for approval as soon as possible afterwards, according to the Criminal Procedure Act Section 210, Second subsection.

As a part of implementing data retention in Norway, the rules regarding access to historical traffic data will change. The Post and Telecom Authority will no longer be a part of the process for individual requests. Instead the initial request must be done to the courts.

## 4.20 Portugal

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

No, it is not.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

Portuguese law on data protection (Law 67/98, of 26 October) does not include, specifically, IP Address in the category of personal data, for the purposes of data protection. It is thus discussed, mainly within data protection and law enforcement communities, if the IP address is, or it is not, personal data.

Portugal ratified Convention 108 of the Council of Europe and transposed to the internal law the EU Directive 95/46/EC. According to both of these instruments, referred into Portuguese Law 67/98, it is considered personal data any information that identifies or leads to the identification of a given person. Thus, the IP address has to be considered personal data.

However, the IP address can be either traffic data (Article 1, 2, d) of Law no 46/2012), as it can identify the device that initiates an electronic communication and the recipient of that communication, and location data (Article 1, 2, e) of Law no 46/2012), as it allows to determine the place where the equipment was used to send or receive an electronic communication.

In both cases, being traffic data or location data, the IP address enables the identification of an individual (the subscriber of the telecommunications service, if a natural person, or the person who on behalf of the legal person subscribed the telecommunications service).

Nevertheless, Portuguese jurisprudence states, in most of the cases, that the IP address has to be considered subscriber information and obtaining it is submitted to the rules of Article 14, number 4 of the Cybercrime Law (Law nº 109/2009, from 15 September) – see below.

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

There is not exactly a legal concept of subscriber information.

However, subscriber is considered "any natural or legal person who is party to a contract with a provider of electronic communications accessible to the public for such services. It is thus natural to deduce that subscriber data are the necessary data in view of the identification of that party of the contract with an electronic communications service.

Besides, Article 14, number 4 of the Cybercrime Law (Law nº 109/2009, from 15 September), includes a list of the types of data that should be considered subscriber data.

Cybercrime Law (Law nº 109/2009, from 15 September)

Article 14

Injunction for providing data or granting access to data

1 - If during the proceedings it becomes necessary for the gathering of evidence in order to ascertain the truth, obtain certain and specific data stored in a given system, the judicial

authority orders to the person who has the control or availability of those data to communicate these data or to allow the access to them, under penalty of punishment for disobedience.

(...)

4 - The provisions of this Article will apply to service providers, who may be ordered to report data on their customers or subscribers, which would include any information other than the traffic data or the content data, held by the service provider, in order to determine:

a) the type of communication service used, the technical measures taken in this regard and the period of service;

b) the identity, postal or geographic address and telephone number of the subscriber, and any other access number, the data for billing and payment available under a contract or service agreement, or

c) any other information about the location of communication equipment, available under a contract or service agreement.

(...)

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

Within a criminal investigation, subscriber information can be obtained only by an order of the Prosecutor (according to Article 14, number 1 and number 4 of the Cybercrime Law (Law n° 109/2009, from 15 September).

That order can be issued if the sought information is needed for "the gathering of evidence in order to ascertain the truth".

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

Obtaining information related to a specific IP address was the same requirements of obtaining subscriber information: can be obtained by an order of the Prosecutor, if that sought information is needed for "the gathering of evidence in order to ascertain the truth" (Article 14, number 1 and number 4 of the Cybercrime Law (Law n° 109/2009, from 15 September).

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

Traffic data is defined under Article 2, c) of the Cybercrime Law (Law n° 109/2009, from 15 September).

Article 2

Definitions

For the purposes of this Law:

(..)

c) "traffic data" means computer data relating to a communication made through a computer system, generated by this system as part of a chain of communication, indicating the origin of the communication, the destination, route, time, the date, size, duration or type of underlying service;

(...)

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

Obtaining traffic data within criminal investigations requires judicial authorization. This authorization can be issued if there are reasons to believe that this is essential to establish the truth or that gathering the evidence would otherwise be impossible or very difficult to obtain by other means. On the other hand, it is limited to serious crimes, as described in Articles 187 and 189 of the Code of Penal Procedure.

## 4.21 Romania

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

The term IP address is not specifically defined in the national legislation.

However, Law no. 304/2003 on universal service and users rights regarding networks and electronic communication services, defines in art.2 lett. f the notion of terminal point of a network as the physical point at which, a subscriber is receiving access to a public communication network; for networks using routing and commutation, the terminal point is identified by a specific network address that can be associated with a number or a name of a subscriber (transposition of the Universal Service Directive 2002/22/EC (network termination point). The same definition is provided by Government Emergency Ordinance no.111/2011 on electronic communications at p.40

**Law no.82/2012 on data retention mentioning the Internet protocol address at:**

- regarding data necessary for tracking or identifying the source of a communication (Art.4 lett. b) p.3) as follows:
  - o Name and address of the subscriber or registered user who was given an IP address, a user identifier or phone number at the moment of a communication
- regarding data necessary for determine date, hour or duration of a communication (Art.6 lett. b) p.1), as follows:
  - o Date and hour when connecting or disconnecting from the internet service, IP address allocated dynamic or static to a communication by the internet service provider, as well as the identifier of the subscriber or of the registered user

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

There is no specific text to say yes or to say no.

However, according to Law no.677/2001 on protection of natural persons with respect to processing of personal data (Data Protection Directive 95/46/EC), for the purpose of this law:

a) **Personal data** represent any information regarding an identified or identifiable natural person; an identifiable natural person is the person who can be identified directly or indirectly, particularly by referring to an identification number or to many specific factors of his physical identity, physiologic, psychic, economic, cultural or social

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

According to **Law no 82/2012** on data retention – **the subscriber** is defined, by **Art.2 lett. c)**, as being the natural or legal person who has a contract with a public electronic communication service provider for providing such a service.

**Art.2 lett. b)**, of the same Law, defines " **the user** " as being the natural or legal person who is using for personally or professionally purposes an electronic communication service for public, and who it is not necessarily a subscriber of that service. A similar definition of "the user" is provided by Law no.506/2004 on protection of personal data against processing of such data during electronic communication.

**Law no.82/2012** defines, for the purpose of its application, the term “**data**” that mean information regarding traffic, location or necessary information to the identification of a subscriber or a user.

The only definition of the term “**user data**” is given by the **Law no.161/2003** which transposed the 2001 CCC into the national legislation and says that by data referring to **user data** is understood any data that can lead to the identification of a user, including the type of communication and the service used, a postal address, geographical address phone numbers or other access numbers and the payment method, any data that can lead to the identification of the user.

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

**Subscriber data** related to a specific electronic communication falls under the provision of the data retention law that means that in order to obtain these data a judge approval is required. During the investigation the request is issued by the prosecutor (Art.152 CPC).

If subscriber data is not related to a specific communication this may be requested by the prosecutor directly from the service provider.

Example of a direct order (art.170 CPC) - What type of service is provided in a location and who is the subscriber?

Example of a request that needs a judge approval – provide subscriber data of a phone number used in November 25th 2013 or an IP address used as the same date.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

The fact the IP address is mentioned as a type of data necessary for tracking or identifying the source of a communication or of data necessary to determine date, hour or duration of a communication (art.4 and 6 of the Law no.82/2012), the subscriber information, related to communication that needs an IP address for being a part of a communication, will fall under the data retention law, that means a judge approval will be needed to get the info (art.152 NCP)

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

***Depending on the domain, traffic data is defined as follows:***

**Law.no 82/2012** (data retention law) – the general definition of **data** includes **traffic information** as well as location or necessary information for the identification of a subscriber or a user.

**Law no.506/2004 art.2 lett. b)** (Law no.506/2004 on protection of personal data against processing of such data during electronic communication) **Traffic data** – any data that is processed for the purpose of transmitting of a communication through an electronic communication network or for purpose of billing.

**Law no.161/2003 art.35 lett. f)** (law transposing the 2001 CC) **Traffic data** – any data referring to a communication done by means of a computer system or produced by, that represent a part of the

communication chain indicating the origin, route, hour, date, size, volume, duration of the communication, as well as the type of the service used for communication

This definition of **traffic data** is in line with the explanation given by the **Explanatory Report** of the 2001 CCC which lists exhaustively the categories of traffic data that are treated by a specific regime which are: the origin of a communication, its destination, route, time (GMT), date, size, duration and type of underlying service. The "**origin**" refers to a telephone number, **Internet Protocol (IP) address**, or similar identification of a communications facility to which a service provider renders services. The "destination" refers to a comparable indication of a communications facility to which communications are transmitted. The term "type of underlying service" refers to the type of service that is being used within the network, e.g., file transfer, electronic mail, or instant messaging.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

The fact that the IP address is mentioned as type of data necessary for tracking or identifying the source of a communication or of data necessary to determine date, hour or duration of a communication (art.4 and 6 of the Law no.82/2012), fall under the data retention law, that means a judge approval will be needed (art.152 NCP).

## 4.22 Serbia

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

Term "IP address" as such is not directly defined but Law on Electronic Communications provides definitions for „address" and "numbers" which can be used for purpose of criminal proceedings as follows:

- Address is a sequence of signs, letters, digits and signals intended to determine the destination of a connection;
- Numbers are series of digits used for addressing in electronic communications networks;
- Internet is a global electronic communications system consisting of a large number of interconnected computer networks and devices exchanging information by using a common set of communication protocols;

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

At the moment there are different approaches with regards to this issue. LEA, Prosecution and other Criminal Justice authorities are not considering IP address as personal data but data which is generated on the basis of subscription contract or other legal binding document. Commissioner for Information of Public Importance and Personal Data Protection on the other hand acknowledges that Ruling of the Constitutional Court of Serbia with regards to the protection of the confidentiality of letters and other forms of communication which rendered unconstitutional certain articles of Law on Electronic Communication, Criminal Procedural Code and Laws on Intelligence Agencies, did not include IP address as such and well, but that the nature of this Ruling, having on mind definition of personal data given by Law on Personal Data Protection, in a broader sense includes IP address as personal data as well.

Personal data is defined as any information relating to a natural person, regardless of the form of its presentation or the medium used (paper, tape, film, electronic media etc.), regardless on whose order, on whose behalf or for whose account such information is stored, regardless of the date of its creation or the place of its storage, regardless of the way in which such information is learned (directly, by listening, watching etc., or indirectly, by accessing a document containing the information etc.) and regardless of any other characteristic of such information.

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

Law on Electronic Communications stipulates that user of electronic communication is a legal or natural entity who uses or requires a publicly available electronic communications service.

Consumer is a physical entity who uses or requires publicly available electronic communications service for personal needs that most ly do not refer to business operations, profession or trade.

Subscriber is any natural or legal entity who or which is a party to a contract with an operator of publicly available electronic communications services for the supply of such services.

Subscriber information is not directly stipulated but regulated through Law provisions on Personal Subscriber Data in the Public Directory (Article 120): The operator providing telephone directory



enquiry services shall notify a subscriber of telephone services, free of charge, about the intention to include his personal data in a publicly available directory of subscribers in printed or electronic form, about its purpose, the availability of personal data through information services, and possibilities of browsing through subscriber personal data by third parties by means of a search engine integrated into the software of the electronic version of the directory. Having received the notification referred to in paragraph 1 of this Article, the subscriber is entitled to refuse to give consent for the inclusion of his/her personal data in the publicly available telephone directory.

The operator from paragraph 1 of this Article shall provide the subscriber whose personal data are in a publicly accessible telephone directory with the possibility to check or correct the data, and the possibility to withdraw the given consent, or to have personal data deleted from the publicly available telephone directory in a simple way and free of charge. The operator referred to in paragraph 1 of this Article shall obtain a subscriber's consent for using the telephone directory for any purpose other than establishing contact with the subscriber on the basis of the subscriber's name and surname or company name or a minimum set of other identity parameters.

The provision of paragraphs 2 and 3 of this Article shall apply to legal entities to the extent in which they are not obliged to make their subscribers' numbers available to the public, whereas the provision of paragraph 4 of this Article shall apply to legal entities without restrictions.

Therefore, subscriber data is defined through service contract between service provider and subscriber.

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

If the public prosecutor cannot assess from the criminal complaint if its assertions are probable, or if the data in the complaint do not provide sufficient grounds to decide whether to conduct an investigation, or if he finds out in some other way that a criminal offence has been committed, the public prosecutor may:

- 1) collect the necessary data himself;
- 2) request citizens [to provide information], under the conditions referred to in Article 288 paragraphs 1 to 6 of Criminal Procedural Code;
- 3) submit a request to public and other authorities and legal persons to provide necessary information.

A responsible person may be fined up to 150,000 dinars for failing to comply with the request of the public prosecutor referred to in paragraph 1 item 3) of this Article, and if after being fined he still refuses to provide the necessary information, another fine in the same amount may be imposed on him once again. The decision on imposing the fine referred to in paragraph 2 of this Article is issued by the public prosecutor.

The police are required to act in accordance with the request of the public prosecutor and to notify him about the measures and actions it had undertaken not later than 30 days from the date of receiving the request.

The public prosecutor, public and other authorities or legal persons, are required during the collection of information or provision of data to act with due care and ensure that no damage is done to the honour and reputation of the person to whom the data relate.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

At the moment, IP address is treated as subscriber information available to Public Prosecution under Criminal Procedural Code provisions, thus specific requirements, other than stated in answer under question number 4 are not required.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

As stipulated by Law on Electronic Communications of Serbia, the operator of public communications networks or the operator of publicly available electronic communications services who processes and keeps traffic data of subscribers and users is under the obligation to erase these data or render the person the data refer to unrecognizable when traffic data cease to be necessary for communications transmission, with the exception of:

- 1) the data necessary for billing services or interconnections, which may be processed until the expiry of the statutory time limit for filing bill complaints or enforcement of collection;
- 2) the data used by the operator for the purpose of marketing and sale of services, with the previously obtained consent of persons the data refer to, and for value added services, to the extent and for the time necessary;
- 3) data withheld pursuant to the provisions of this Law.

Prior to the commencement of traffic data processing from paragraph 1 item 1) of this Article and prior to obtaining the consent referred to in paragraph 1 item 2) of this Article, the operator shall inform the subscriber or user about the types of traffic data which shall be processed and the duration of such processing. The person who has given consent for data processing referred to in paragraph 1 item 2) of this Article may withdraw such consent at any time.

The processing of traffic data referred to in paragraph 1 of this Article shall be conducted only by persons who, for the needs of operators, handle billing or network management, customer questions, fraud detection, marketing and sale of electronic communications services, and provide value added services, to the extent necessary for carrying out the abovementioned activities. The provisions of paragraphs 1 and 4 of this Article shall not apply to the competencies of the Agency and other relevant state authorities to obtain insight into network traffic data, of significant relevance to dispute resolution, especially in relation to service billing or interconnection disputes.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

Court order must be issued prior to obtaining traffic data.

## 4.23 Slovakia

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

National (criminal) law does not define *expressis verbis* a term "IP address". However, the Ministry of Finance of the Slovak Republic with a view to ensure the unification during the process of defining the terms for the area of informatization of society published a methodical instruction which defines the above-mentioned term (on the basis of the Act No. 275/2006 Coll. on the information systems of the public administration and to amend and supplement certain acts as amended by Act No. 678/2008 Coll.).<sup>12</sup>

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

An IP address is considered for personal data. Since it is possible in certain cases to derive from the IP address an identity of a person, on the basis of the provisions of Section 5 of the Decree of the Ministry of Justice of the Slovak Republic No. 482/2011 Coll. on the Publication of the Judicial Decisions. The IP address along with other data is subject to anonymization also within the publication of the judicial decisions, when it is considered with other relevant data for personal data.<sup>13</sup>

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

The categories of obtained/acquired and processed data are regulated in the provisions of Section 56 par. 3 of Act No. 351/2011 Coll. on Electronic Communications as amended.<sup>14</sup>

---

<sup>12</sup> Art. 2 (Glossary of terms) of Methodical instruction on the Use of the Special Terms for the Area of Informatization of Society (published in the Financial rapporteur No. 42/2008):  
*An IP address is a numeric identifier of a subject for TCP/IP networks, enabling communication of several parties in the network. The connection of a private network to Internet requires a use of registered IP addresses in order to prevent from duplicity.*

<sup>13</sup> Section 5 par. 1 of the Decree of the Ministry of Justice of the Slovak Republic No. 482/2011 Coll. on the Publication of the Judicial Decision:

(1) Data which are subject to anonymization are:

- a) birth number,
- b) date of birth,
- c) number of ID card, passport or other document proving identity of a person,
- d) residence,
- e) telephone number, fax number, e-mail address, IP address, URL address,
- f) name and code of the bank or branch of a foreign bank, bank account number, account name, IBAN, client number,
- g) indication of the cadastral area,
- h) number of property sheet,
- i) classified information and trade secret,
- j) name and surname of a natural person, if it does not refer to natural person in par. 2,
- k) names and surnames of legal representatives of participants and parties in proceedings and guardians of participants and parties in proceedings, parties in proceedings, other persons participating in proceedings.

<sup>14</sup> Section 56 par. 3 of Act No. No. 351/2011 Coll. on Electronic Communications as amended:

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

The requirements which have to be met in order to obtain subscriber information from a service provider are regulated in the provisions of Sections 90, 115 116 of the Slovak Code of Criminal Procedure (Act No. 301/2005 Coll. as amended). The Slovak Code of Criminal Procedure (Act No. 301/2005 Coll. as amended) within the definitions of certain terms does not differ between the process of obtaining requirements concerning subscriber information and obtaining traffic data. The provision of Section 10 par. 21 of the Slovak Code of Criminal Procedure (Act No. 301/2005 Coll. as amended) defines information-technical means which are determined to obtain data. The Slovak Code of Criminal Procedure (Act No. 301/2005 Coll. as amended) differ data only in the sense as it comes out of the terms which can be derived from the provisions of Sections 90, 115 and 116 of the Slovak Code of Criminal Procedure (Act No. 301/2005 Coll. as amended).

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

-

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

The requirements which have to be met in order to obtain traffic data from a service provider are regulated in the provisions of Sections 90, 115 and 116 of the Slovak Code of Criminal Procedure.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

The Slovak Code of Criminal Procedure (Act No. 301/2005 Coll. as amended) does not differ between subscriber information and traffic data. The concrete requirements are provided in Sections 10 (par.21), 90, 115 and 116 of the Slovak Code of Criminal Procedure (Act No. 301/2005 Coll. as amended).

---

*An enterprise providing public services may for the purposes of the conclusion and implementation of contracts for the provision of public services, its amendment, termination or porting of a number, billing, receiving and recording of payments, claims and cession of claims and elaboration of a list of participants obtain and process data of participants which are a phone number, an amount of unpaid commitments and*

- a) name, title, address of permanent residence, birth number, identity card number or number of other identity document of a natural person, nationality,*
- b) business name, place of business and identification number of a natural person-entrepreneur or*
- c) business name, seat and identification number of a legal person."*

## 4.24 Slovenia

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

No, the term IP address is not defined in Slovenian legislation.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

IP address is not defined as personal data in Slovenian legislation. There is no uniformly opinion on this.

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

They are defined in Electronic Communication Act (article 110):

- personal name or business name of the client
- address of the subscriber;
- subscriber number or other elements numbering used for establishing the connection to the client;
- academic, scientific or professional name of the client or his e-mail address (available on subscribers request);
- tax number for persons, and tax and registration number for firms

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

Police must have grounds for suspecting criminal act. These information can be obtain with Police formal letter (Criminal Procedure Code, article 149b/III).

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

If the IP address is static then the subscriber information can be obtain with Police formal letter. If the IP address is dynamic then it is part of traffic data, so the subscriber information must be obtain only with court order (Criminal Procedure Code, article 149b/I). In both cases police must have grounds for suspecting criminal act.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

They are defined in Electronic Communication Act (article 3, definition no. 25):

Traffic data contain information relating to the:

- routing, duration, time or volume of communication,
- protocol used,
- location of the terminal equipment of the sender or recipient,
- network on which the communication originates or terminates,

- beginning, end or duration of a connection.

They may also contain the format in which the message is transmitted by means of its network.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

Police must have grounds for suspecting criminal act. Traffic data must be obtained only with court order (Criminal Procedure Code, article 149b/I).

## 4.25 Spain

**Question 1: Is the term “IP address” defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

There is no legal concept for IP-address (Internet Protocol) within the Spanish legislation.

However, Article 3.1 a) 2 of Law 25/2007, of 18 October,<sup>15</sup> on the Retention of Data concerning Electronic Communications and Public Communication Networks, makes explicit reference to IP-

---

<sup>15</sup> Article 3 of the Law on Data Retention: Data to be retained

1. Data that should be retained by operators specified in Article 2 of this Law are as follows:

- a) Data necessary to trace and identify the source of a communication:
  1. Concerning fixed network telephony and mobile telephony:
    - i) The calling telephone number
    - ii) The name and address of the subscriber or registered user.
  2. Concerning Internet access, Internet E-mail and Internet telephony:
    - i) The user ID allocated
    - ii) The user ID and telephone number allocated to any communication entering the public telephone network
    - iii) The name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication
- b) Data necessary to identify the destination of a communication:
  1. Concerning fixed network telephony and mobile telephony:
    - i) The number or numbers dialed (destination phone number or numbers) and, in cases involving other services such as call forwarding or call transfer, the number or numbers to which the calls are routed
    - ii) The names and addresses of subscribers or registered users
  2. Concerning Internet E-mail and Internet telephony:
    1. i) The user ID or telephone number of the intended recipient(s) of an Internet telephony call
    2. ii) The names and addresses of subscribers or registered users and user ID of the intended recipient of the communication
- c) Data necessary to identify the date, time and duration of a communication:
  1. Concerning fixed network telephony and mobile telephony: the date and time of the start and end of the call or, where appropriate, of the messaging or multimedia service
  2. Concerning the access to Internet, Internet E-mail and Internet telephony:
    - i) The date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet service provider to a communication, and the user ID of the subscriber or registered user
    - ii) The date and time of the log-in and log-off of the Internet E-mail service or Internet telephony service, based on a certain time zone
- d) Data necessary to identify the type of communication:
  1. Concerning fixed network telephony and mobile telephony: the phone service used: type of call (voice transmission, voicemail, conference call, data call), supplementary services (including call forwarding or transfer) or messaging or multimedia services employed (including short message service, advanced multimedia services and multimedia services)
  2. Concerning Internet E-mail and Internet telephony: the Internet service used.
- e) Data necessary to identify the user's communication equipment or what purports to be their equipment:
  1. Concerning fixed network telephony; the calling and called telephone numbers

addresses linked to a communication considering them data to be retained by communication operators and to be left at the disposal of judicial authorities in the event they are needed in the course of a criminal investigation. In order to have access to this information stored by communication operators, a duly motivated authorization would be required, issued by the competent judicial authority that is carrying out a criminal investigation of a serious offence.

In view of bringing clarification to certain doubts raised on the need of judicial authorization to have access to IP-addresses linked to a communication process, it is worth noting that the Second Division of the Supreme Court, in its Plenary Meeting of 23 February 2010, adopted the following agreement: "*A judicial authorization should be required by operators rendering electronic communication or public communication network services before transferring data generated or processed to that end. Therefore, the Public Prosecutor shall need such authorization to obtain from operators data retained within the meaning of Article 3 of Law 25/2007, of 18 October*".

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

According to Article 3.a) of the Organic Law 15/1999, of 13 December, on the Protection of Personal Data (LOPD), personal data means: "*any information concerning an identified or identifiable natural person*". At the same time, the Regulations of this Law, published by Royal Decree 1720/2007, of 21 December, under its Article 5.1.f), defines personal data as "*Any numerical, alphabetical, graphic, photographic, acoustic or other kind of data concerning an identified or identifiable natural person*". On the basis of these definitions and since it is obvious that IP on its own does not make it possible to identify a natural person without further information, the doubt was raised on whether such data would, nevertheless, facilitate identification and therefore, if it should be included within the concept "identifiable" used by the LOPD.

In order to resolve that issue, the Spanish Data Protection Agency (AEPD) considered in its Report 327/2003 that "*IP addresses, both fixed and dynamic, irrespective of the type of access, must be considered personal data*". The AEPD's reasoning in support of the above is that each TCP/IP network has a unique IP address, both for the sender's and the recipient's computers, and when this data is linked with other information, such as the domain name allocated to each computer, the date and time of the allocation of the specific address or the subscriber's ID, it is possible to get to know the

- 
2. Concerning mobile telephony:
    - i) The calling and called telephone numbers
    - ii) The international Mobile Subscriber Identity (IMSI) of the calling party
    - iii) The International Mobile Equipment Identity (IMEI) of the calling party
    - iv) The IMSI of the called party
    - v) The IMEI of the called party
    - vi) In the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated
  3. Concerning Internet access, Internet E-mail and Internet telephony:
    - i) the calling telephone number for dial-up access
    - ii) the digital subscriber line (DSL) or other end point of the originator of the communication
  - f) data necessary to identify the location of mobile communication equipment:
    - 1) the location label (Cell ID) at the start of the communication
    - 2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2 No data revealing the content of the communication may be retained pursuant to this Law.



name of the legal entity or natural person that is the holder of the IP address or the identity of the specific user to whom a particular IP address has been allocated.

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

In Annex II to the General Telecommunications Law (LGT) a subscriber is defined as any legal or natural person which or who is party to a contract with the provider of publicly available telecommunications services for the supply of such services.

According to Circular 1/2013 of the Spanish Commission for the Telecommunications Market on the procedure for delivering and receiving subscriber's data, the following should be considered personal subscriber information:

- Identification of the holder
- Natural person: name and surname, Identity Card, Tax Identification, Foreigner Identification or Passport Number
- Legal person: Company name, Tax Identification Number, Trade name
- Identification of the user
  - Similar data as for natural and legal persons
- Full address (postal identification of the subscriber)
- Subscriber number (ranges and/or individual numbers)
  - List of numbers assigned to the postal address
- Consent to the publication of data or to their use with commercial or advertising purposes
- Type of terminal, where appropriate
- Method of payment
- Operator

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

Please see next answer.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

Article 34.2 of the General Telecommunications Law (LGT) establishes the obligation of operators to ensure the levels of data protection required by Organic Law 15/1999 of 13 December on Protection of Personal Data (LOPD). In the same sense, paragraph 3 of Article 38 of such law lays down the subscribers' privacy rights and paragraph 6 – by regulating the data assignment for the development of directories of subscribers – expressly states that in any case the right to protection of personal data shall be ensured; therefore, the retention and processing of the subscriber information shall be carried out according to the legislation on data protection.

Pursuant to the provisions of Article 11 of the LOPD, personal data can only be communicated to third parties if there is previous consent of the interested party, though such consent is not necessary for the exemptions set out in such article, one of those is the following:

Article 11.2 F) *When the communication to be conveyed is addressed to the Ombudsman, the Office of the Public Prosecutor or Judges and Courts or the Court of Audit within the scope of the functions expressly assigned to them.*

Thus, the judicial authority can obtain the subscriber information, in any case, in the course of criminal investigations in accordance with Article 18 of the Spanish Constitution and with the specific regulations abovementioned.

The Public Prosecution may do so on the basis of the provisions of Article 11 2 F) of the LOPD aforementioned, unless such information is subject to confidentiality of communications, in which case a judicial authorization shall always be required or when, according to a specific regulation or when it affects the right of intimacy, such judicial authorization shall be likewise required.

As for the Law Enforcement Agencies, both the Spanish Constitutional Court and the Supreme Court have traditionally understood that when the access to that information does not affect the secrecy of communications but only the right of personal privacy and in exceptional cases of necessity and urgency, they could possibly accede to such information in the exercise of their legal functions of investigation and prevention of crime, detection of criminals and tools, effects and evidence collection, based on Articles 282 of the Criminal Procedure Code, Article 11.1 of Organic Law 2/1986 of 13 March on Law Enforcement Agencies and Article 14 of Organic Law 1/1992 of 21 February on the Protection of Citizens' Security.

However, the publication of Law 25/2007 of 18 October on the Retention of Data concerning Electronic Communications has had a great impact on this issue. This law obliges the operators providing electronic communications services to preserve certain data (subscriber information, among them) generated and processed within the framework of the provision of that service and specifically those foreseen in Article 3 of such Law, as data necessary:

- a) *To trace and identify the source of a communication.*
- b) *To identify the destination of a communication.*
- c) *To determine the date, time and duration of a communication.*
- d) *To identify the type of a communication.*
- e) *To identify the users' communication equipment or what purports to be their equipment.*

As regards the subscribers' data referred to in Article 3, Article 1<sup>16</sup> of Organic Law 25/2007 establishes a special regime according to which data can only be supplied by operators at the request of the judicial authority at the time of the investigation of a serious criminal offence. The data delivery shall be carried out by the authorised officers mentioned in Article 6<sup>17</sup> of the same legal text.

---

<sup>16</sup> Article 1.

**1.-** *This law is intended to regulate the operators' obligation to retain data generated or processed within the framework of the provision of electronic communications services or of public communications networks as that of the assignment of such data to authorised officers whenever requested through the relevant judicial authorization for the purposes of detection, investigation and prosecution of serious criminal offences as referred to in the Criminal Code or in special criminal laws.*

**2.-** *This law shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user.*

**3.-** *This law shall not apply to the content of electronic communications, including information consulted using an electronic communications network.*

<sup>17</sup> Article 6 of this Law also considers authorised officers:

a) *The members of the Law Enforcement Agencies in the exercise of criminal police duties, pursuant to the provisions of Article 547 of the Organic Law 6/1985 of the Judiciary, of 1 July.*

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

Royal Decree 424/2005 of 15 April, approving the Regulation about the conditions to give services of electronic communications, the universal service and the users' protection, defines traffic data in its Article 64.a) as *any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*.

The same article in its paragraph c) defines *communication as any information exchanged or transmitted between a finite number of interested parties by means of a publicly available electronic communications service*.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

According to the case-law of the Supreme Court and the Constitutional Court, the fundamental right to confidentiality of communications set out in Article 18.3<sup>18</sup> of the Spanish Constitution covers not only the content of communications but also those traffic data linked to such communications. Therefore, judicial authorization shall be needed in any case to get access to such information except with the consent of the interested party.

As mentioned above, the access to traffic data retained by telecommunications operators is regulated by the abovementioned provisions of Law 25/2007, of 18 October, on the retention of data concerning electronic communications and public communications networks, according to which, as expected, a judicial authorization issued in the course of a criminal investigation for a serious offence is required.

Even though the consideration of a serious offence has been traditionally linked not only to the appropriate penalty for the criminal offence committed but also to other factors such as the legal interest protected, the significance of the behaviour or the action of organized crime groups, recently some doctrinal arguments have been raised regarding such concept. However it is predictable that the on-going procedural reforms can definitively solve these differences of opinion.

---

b) Assistant Directorate-General for Customs Surveillance's officers in the exercise of their powers as criminal police force, as provided for in paragraph 1 of Article 283 of the Code of Criminal Procedure.

c) The National Intelligence Centre's staff in the course of security investigations on persons or entities, according to the provisions of Law 11/2002 of 6 May, regulating the National Intelligence Centre and, to the provisions of the Organic Law 2/2002 of 6 May, regulating the National Intelligence Centre's prior judicial review.

<sup>18</sup> Article 18.3 guarantees the right to confidentiality of communications, particularly communications by post, telegraph and telephone.

#### 4.26 "The former Yugoslav Republic of Macedonia"

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

No.

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

No, if it is an dynamic IP address, but if it is static IP address, then that is an personal data, regarding the Law for protecting personal data (Art. 2 P.1 , personal data can be determine as:

"Personal information" is any information which relates to identified individual or physical person may be identified, and a person who can identify a person whose identity can be determined directly or indirectly, in particular on the basis of unique identification number of the citizen or based on one or more features specific to his physical, mental, economic, cultural or social identity;

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

According to the Law for electronic communications (Art. 4 Paragraph 8): User identification code means unique identification code assigned to the subscriber or registered user to access the service internet for communication or online service.

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

It depends on the phase of the procedure, because if it is the pre investigation and investigation phase, than the request for a data from the public prosecutor to the judicial police it's enough for gathering information from the ISP-S (Article 287 paragraph 8 from CPC ).

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

It depends on the phase of the procedure, because if it is the pre investigation and investigation faze, than the request for a data from the public prosecutor to the judicial police it's enough for gathering information from the ISP-S (Article 287 paragraph 8 from CPC ). And If we need the searching, than we use the Art. 184 from the CPC :

Searching in the computer system and computer data

( 1 ) At the request of the person executes the warrant , who uses a computer or have access to it or to another device or data carrier , shall enabling - Walkthrough access to them and give them the necessary information for smooth accomplishment of the purpose of the hearing .

( 2 ) At the request of the person executes the warrant who uses a computer or have access to it or other device or data subject shall immediately take measures to prevent ruining - or changing data .

( 3 ) A person who uses a computer or access to it or to another device or carrier of Data and who shall not act in paragraphs ( 1 ) and ( 2 ) the this article, and that there are no justified reasons , the judge of the previous procedure can penalty under the provisions of Article 88 paragraph ( 1 ) of this Law .

Art. 198 from CPC

Temporary confiscation of computer data

( 1 ) The provisions of Articles 194 paragraph ( 1 ) , paragraph 195 ( 1 ) and 197 of this Law shall apply to the data stored in the computer and related devices for automatic, or electronic data processing devices used for the collection and transmission of data carriers data and subscriber information that provider . Upon written request of the Public Prosecutor, these data must be delivered the public prosecutor in the term he chose.

In case of refusal, it shall proceed under Article 196, paragraph ( 1 ) of this Act .

( 2 ) A judge of the preliminary procedure proposed by the Attorney General may issue to determine protection and storage of computer data under Article 185 of this law until it is needed , and the longest six – month after this period, the data will be returned ,unless they are involved in such criminal work damage and unauthorized intrusion into computer system under Article 251 of the Computer Fraud Article 251 - B and Computer fraud under Article 379 - and all of the Criminal Code, if not included in the another crime with the help of computer, and if they do not serve as evidence of a crime .

( 3 ) The decision of the judge of the previous procedure which measures specified in paragraph ( 2 ) of this Article , the person who uses the computer and the person which service provider is entitled to appeal within 24 hours. The appeal to the council under Article 25 paragraph ( 5 ) of this Act . The appeal does not suspend the enforcement of the decision .

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text**

Under the provisions of the Criminal code Art. 122 Paragraph 27 the traffic data is defined as: Computer data shall refer to presenting facts, information or concepts in format suitable for procession via a computer system, including program favourable for putting the computer system in function.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

Order from the Public prosecutor is needed for obtaining the needed information.

## 4.27 Ukraine

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

Yes, the term "IP address" defined in Ukrainian law of Telecommunications (article 1 of this law):

- **subscriber number** - a set of digits for marking (identification) of terminal equipment of a subscriber in telecommunications network
- **address on the Internet** - determined by the current online international standards numeric and / or symbolic identifier Domain names in the hierarchical Domain Name System
- **абонентський номер** - сукупність цифрових знаків для позначення (ідентифікації) кінцевого обладнання абонента в телекомунікаційній мережі;
- **адреса мережі Інтернет** - визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символічний ідентифікатор доменних імен в ієрархічній системі доменних назв;

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

No, only the information about the person that placed at provider of telecommunications related to personal data and data that contain legally protected secrets. It's defined in Ukrainian criminal Procedure code. (article 162 item 7)

Стаття 162. Речі і документи, які містять охоронювану законом таємницю

7) інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо;

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

3) The information contained in the telecommunication carriers and providers, the relationship, the person providing telecommunications services, including those receiving services, their duration, content, routes of transmission, etc.

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

The sides of criminal proceedings may apply to the investigating judge during the preliminary investigation or the court proceedings during the request for temporary access to objects and documents, except as provided in article 161 of Ukrainian criminal Procedure code. An investigator may apply for petition in agreement with the prosecutor.

Стаття 160. Клопотання про тимчасовий доступ до речей і документів

1. Сторони кримінального провадження мають право звернутися до слідчого судді під час досудового розслідування чи суду під час судового провадження із клопотанням про тимчасовий

доступ до речей і документів, за винятком зазначених у [статті 161](#) цього Кодексу. Слідчий має право звернутися із зазначеним клопотанням за погодженням з прокурором.

Стаття 161. Речі і документи, до яких заборонено доступ

1. Речами і документами, до яких заборонено доступ, є:

- 1) листування або інші форми обміну інформацією між захисником та його клієнтом або будь-якою особою, яка представляє його клієнта, у зв'язку з наданням правової допомоги;
- 2) об'єкти, які додані до такого листування або інших форм обміну інформацією.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

The application shall include:

- 1) a summary of the circumstances of a criminal offense in connection with which the petition is filed;
- 2) the legal qualification of the criminal offense indicating article (part of the article) of the Law of Ukraine on criminal liability;
- 3) The items and the documents, temporary access is planned to obtain;
- 4) suggests that things and documents are or may be in the possession of the person or entity;
- 5) the value of things and documents to establish the circumstances of the criminal proceedings;
- 6) the use as evidence of information contained in the documents and things, and other ways to prove the impossibility of the circumstances that are intended to prove through these things and documents in the case of an application for temporary access to objects and documents that contain secrets protected by law;
- 7) the rationale for removal of items and documents, unless the issue violated party to the criminal proceedings.

У клопотанні зазначаються:

- 1) короткий виклад обставин кримінального правопорушення, у зв'язку з яким подається клопотання;
- 2) правова кваліфікація кримінального правопорушення із зазначенням статті (частини статті) закону України про кримінальну відповідальність;
- 3) речі і документи, тимчасовий доступ до яких планується отримати;
- 4) підстави вважати, що речі і документи перебувають або можуть перебувати у володінні відповідної фізичної або юридичної особи;
- 5) значення речей і документів для встановлення обставин у кримінальному провадженні;
- 6) можливість використання як доказів відомостей, що містяться в речах і документах, та неможливість іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів, у випадку подання клопотання про тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю;
- 7) обґрунтування необхідності вилучення речей і документів, якщо відповідне питання порушується стороною кримінального провадження.

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text**

**Traffic** - a set of information signals transmitted by technical means operators and providers telecommunications at a certain interval of time, including information data user and / or proprietary information.

**Трафік** - сукупність інформаційних сигналів, що передаються за допомогою технічних засобів операторів, провайдерів телекомунікацій за визначений інтервал часу, включаючи інформаційні дані споживача та/або службову інформацію;

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

7) The same answer that in question 5.



## 4.28 USA

**Question 1: Is the term "IP address" defined for criminal law purposes in your domestic legislation (criminal or regulatory or technical laws or regulations etc.)? If yes, please provide the text of the law or regulation.**

—  
No, "IP address" is not specifically defined for criminal law purposes. Instead, an IP address falls within other categories of protected information. For example, the IP address assigned to a subscriber is protected as "a record or other information pertaining to a subscriber." 18 U.S.C. §§ 2702(a)(3), 2703(c)(1). In addition, United States law permits investigators to use a subpoena to obtain the "telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address" of a customer or subscriber." 18 U.S.C. § 2703(c)(1)(E). Under this provision, an IP address is a "subscriber number or identity."

**Question 2: Is an IP address considered to be personal data? If yes, please provide the relevant text.**

—  
Yes. Except in limited circumstances, such as an emergency, United States law prohibits an ISP from disclosing subscriber IP addresses to the government without legal process. As noted above, an IP address is a record or other information pertaining to a subscriber, and that information is protected by statute. See 18 U.S.C. § 2702(a)(3) ("a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.").<sup>19</sup>

**Question 3: What categories of data are considered subscriber information under your domestic law? Please provide the text.**

—  
Although United States law does not use the phrase "subscriber information," it specifies certain categories of basic information about a subscriber that the government may obtain using a subpoena. In particular, the government may use a subpoena to obtain the "(A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number)" of a subscriber. 18 U.S.C. § 2703(c)(2).

**Question 4: Which requirements must be met so that the police or judicial authority can obtain subscriber information from a Service Provider within a criminal investigation?**

Investigators may use a subpoena to obtain the basic subscriber information described in question 3 above. Investigators must use a court order or a court-issued warrant to obtain any additional detailed non-content information about a subscriber.

---

<sup>19</sup> NB: "personal data" is used here in the context of American criminal law. This is not necessarily comparable to its use in European data protection law.

**Question 5: Specifically, which requirements must be met so that the police or judicial authority can obtain the subscriber information for a specific IP address within a specific criminal investigation?**

—  
To obtain the subscriber assigned to an IP address, or the IP address assigned to a subscriber, investigators may use a subpoena. See 18 U.S.C. § 2703(c)(2). In addition, they may use a court order or court-issued warrant. See 18 U.S.C. § 2703(c)(1).

**Question 6: What categories of data are considered traffic data under your domestic law? Please provide the text.**

—  
Although United States criminal law does not use the phrase “traffic data,” it includes a provision for all non-content information: “a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications).” 18 U.S.C. § 2703(c)(1). In addition to basic subscriber information, this category includes address information of others with whom a subscriber communicates, including email addresses and IP addresses.

**Question 7: Which requirements must be met so that the police or judicial authority can obtain traffic data from a Service Provider within a criminal investigation?**

To compel disclosure of traffic data, investigators must use either a search warrant (a court order issued on a factual showing of probable cause), or a court order issued on a showing of “specific and articulable facts” that the records sought are “relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(c)(1), (d).

Excerpts of the relevant statutes are attached.

## 5 Appendix: Additional information provided

### 5.1 Canada

Supreme Court of Canada: R v. Spencer (June 2014)<sup>20</sup>

Constitutional law — [Charter of Rights](#) — Search and seizure — Privacy — Police having information that IP address used to access or download child pornography — Police asking Internet service provider to voluntarily provide name and address of subscriber assigned to IP address — Police using information to obtain search warrant for accused's residence — Whether police conducted unconstitutional search by obtaining subscriber information matching IP address— Whether evidence obtained as a result should be excluded — Whether fault element of making child pornography available requires proof of positive facilitation — [Criminal Code, R.S.C. 1985, c. C46](#) , [ss. 163.1\(3\)](#) , [163.1\(4\)](#) , [487.014\(1\)](#) — [Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5](#) ,[s. 7\(3\)](#) (c.1)(ii) — Charter of Rights and Freedoms, s. 8.

### 5.2 Finland

- Act on the Exercise of Freedom of Expression in Mass Media
- Act on the Protection of Privacy in Electronic Communications
- Coercive Measures Act
- Criminal Investigation Act
- Personal Data Act
- Police Act

### 5.3 Norway

Forskrift om lagringsplikt for bestemte data og om tilrettelegging av disse data (datalagringsforskriften)

### 5.4 USA

#### **§2702. Voluntary disclosure of customer communications or records**

(a) Prohibitions.—

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications ...) to any governmental entity.

#### **§2703. Required disclosure of customer communications or records**

(c) Records Concerning Electronic Communication Service or Remote Computing Service.—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

- (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure ... by a court of competent jurisdiction;
- (B) obtains a court order for such disclosure under subsection (d) of this section;
- (C) has the consent of the subscriber or customer to such disclosure;
- (D) ...; or

---

<sup>20</sup> <http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do>

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

- (A) name;
- (B) address;
- (C) local and long distance telephone connection records, or records of session times and durations;
- (D) length of service (including start date) and types of service utilized;
- (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
- (F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal ... statute or a Federal ... grand jury or trial subpoena or any means available under paragraph (1).

(d) Requirements for Court Order.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. ... A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

## **6 Annexe: extraits de la Convention de Budapest**

### **Article 1 – Définitions**

Aux fins de la présente Convention,

- a l'expression «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;
- b l'expression «données informatiques» désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;
- c l'expression «fournisseur de services» désigne:
  - i toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et
  - ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.
- d «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

### **Article 18 – Injonction de produire**

- 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:
  - a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et
  - b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.
- 2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.
- 3 Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

- a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;
- b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;
- c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

### **Rapport explicatif – extraits**

177. L'expression 'informations relatives aux abonnés' est définie au paragraphe 3. En principe, elle désigne toute information détenue par l'administration d'un fournisseur de services et qui se rapporte à un abonné à ses services. Les données relatives aux abonnés peuvent être contenues sous forme de données informatiques ou sous toute autre forme, telle que des documents-papier. Comme les informations relatives aux abonnés ne se présentent pas toutes sous la forme de données informatiques, une disposition spéciale a été insérée dans l'article pour tenir compte de ce type d'informations. Le terme d'« abonné » vise à englober de nombreuses catégories de clients des fournisseurs de services : personne ayant payé un abonnement, client qui paie au fur et à mesure les services qu'il utilise, personne bénéficiant de services gratuits. Sont aussi incluses les informations concernant les personnes habilitées à utiliser le compte de l'abonné.

178. Dans le cadre d'une enquête pénale, les informations relatives aux abonnés peuvent être nécessaires dans deux situations spécifiques. Premièrement, elles sont nécessaires pour déterminer les services et mesures techniques connexes qui ont été utilisés ou sont utilisés par un abonné, tels que le type de service téléphonique utilisé (par exemple téléphonie mobile), le type de services connexes utilisé (renvoi automatique d'appel, messagerie téléphonique, etc.), le numéro de téléphone ou toute autre adresse technique (comme une adresse électronique). Deuxièmement, lorsqu'une adresse technique est connue, les informations relatives aux abonnés sont requises pour aider à établir l'identité de l'intéressé. D'autres informations relatives aux abonnés, telles que les informations commerciales figurant dans les dossiers de facturation et de paiement de l'abonné, peuvent également être utiles aux enquêtes pénales surtout lorsque l'infraction faisant l'objet de l'enquête concerne un cas de fraude informatique ou un autre délit économique.

179. En conséquence, les informations relatives aux abonnés recouvrent différents types d'informations sur l'utilisation d'un service et l'utilisateur de ce service. S'agissant de l'utilisation du service, l'expression désigne toute information, autre que des données relatives au trafic ou au contenu, permettant d'établir le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période pendant laquelle l'intéressé a été abonné au service en question. L'expression 'dispositions techniques' désigne l'ensemble des mesures prises pour permettre à l'abonné de profiter du service de communication offert. Ces dispositions incluent notamment la réservation d'un numéro ou adresse technique (numéro de téléphone, adresse de site Web ou nom de domaine, adresse électronique, etc.) ainsi que la fourniture et l'enregistrement du matériel de communication utilisé par l'abonné (appareils de téléphonie, centres d'appel ou réseaux locaux).

180. Les informations relatives aux abonnés ne sont pas limitées aux informations se rapportant directement à l'utilisation du service de communication. Elles désignent également toutes les informations, autres que des données relatives au trafic ou au contenu, qui permettent d'établir

l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'utilisateur, et tout autre numéro d'accès et les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou arrangement de service entre l'abonné et le fournisseur de services. Elles désignent en outre toute autre information, autre que des données relatives au trafic ou au contenu, relative à l'endroit où se trouvent les équipements de communication, information disponible sur la base d'un contrat ou arrangement de service. Cette dernière information peut n'avoir d'intérêt pratique que dans le cas d'équipements non portatifs, mais le fait de savoir si les équipements en question sont portatifs ou de connaître l'endroit où ils se trouveraient (sur la base de l'information fournie en vertu du contrat ou de l'arrangement de service) peut être utile à l'enquête.

181. Cet article ne fait toutefois pas obligation aux fournisseurs de services de conserver des données sur leurs abonnés. Et les fournisseurs ne seront pas non plus tenus, en vertu de la Convention, de s'assurer de l'exactitude desdites données. En d'autres termes, les fournisseurs de services ne sont pas astreints à enregistrer les données relatives à l'identité des utilisateurs des télécartes donnant accès aux services radiotéléphoniques mobiles. Ils ne sont pas non plus obligés de vérifier l'identité des abonnés ou de s'opposer à l'emploi de pseudonymes par les utilisateurs de leurs services.

182. Les pouvoirs et procédures faisant l'objet de la présente section étant instaurés aux fins d'enquêtes ou de procédures pénales spécifiques (article 14), les injonctions de produire sont appelées à être utilisées dans des affaires individuelles concernant le plus souvent un abonné. Ainsi, par exemple, sur la base de la mention du nom de telle ou telle personne dans l'injonction de produire, un numéro de téléphone ou une adresse électronique peuvent être demandés. Sur la base d'un certain numéro de téléphone ou d'une certaine adresse électronique, le nom et l'adresse de l'abonné peuvent être demandés. La mention susvisée n'autorise pas les Parties à rendre une ordonnance aux fins de divulgation de quantités non sélectives d'informations relatives aux abonnés par un fournisseur de services relatives à des groupes d'abonnés, par exemple aux fins d'extraction de données.