|  |  |
| --- | --- |
| **Council Working Group on International Internet Related Public Policy issues (CWG-Internet) Twelfth meeting – Geneva, 1 February 2019** |  |
|  |  |
|  |  |
|  | **Document WG-Internet 12/4-E** |
| **17 January 2019** |
| **English only** |

Contribution by the Russian Federation

practice of establishing ott services regulatory mechanisms and proposals on the cooperation OF all stakeholders on Cross-industry and international level

1. **Introduction**

Rapid development of the information and communication technologies (ICTs) has led to wide distribution of Internet-provided services, also known as OTT services.

Such services have a considerable impact on national and international telecommunications and became an important part of global digital economy. In this regard, the international public policy considerations related to OTT should be reviewed comprehensively and include such issues as security, privacy, personal data protection, measures to prevent illegal use, etc. OTT services development raises new challenges for telecommunication industry regulation that should also focus on promoting investment and innovations. In many countries there is already an established practice for regulation of OTT services, which is worth considering for the purposes of sharing the best practices, and worth analyzing for developing, if needed, recommendations and/or other CWG-Internet output documents.

1. **Discussions**

First of all, it is worth noting that OTT services combine multiple services in various areas having several common features:

* The use of IP protocol packet switched networks for information transmission;
* Provision of services independently from an operator providing the access to the Internet (over-the-top of the network);
* Traditional telecommunication and innovation services to be provided on a free or freemium basis which does not require service providers to sign contrasts and receive payment from users;
* Services are monetized through advertisement and/or partner services, which requires contractual obligations only with the partner;
* Services provided on a cross-border basis.

An important aspect that should be taken into account when considering the regulation approaches to OTT services is their cross-border nature which requires collaboration and coordination between the States and all stakeholders on an international level.

OTT services play an important role in telecommunications/ICTs at the national and international levels as well as raise new challenges before regulatory authorities related to promoting investment and innovation, security aspects, privacy, personal data protection, etc.

The document below (see the Annex) presents the examples OTT services’ regulation by various countries. The given examples do not cover fully this issue but they present a sufficient picture on the extensiveness of OTT regulatory practices development. The matters pertaining to regulation of services provided within a particular Internet service, as well as usage of this service is subject to national responsibility and constitute a sovereign right of any state. However, taking into account the cross-border nature of Internet services, it is worth noting that OTT regulation will be more successful should Member States coordinate their efforts at the national level, besides establishing the international regulation. Russian Administration is deeply concerned with the lack of regulation of Internet services at the international level, particularly the OTT, which leads to Internet fragmentation (meaning the establishment of national and regional areas with various set of services and working conditions), new hurdles emerging preventing the establishment of the favourable environment of Internet development.

CWG–Internet conducted online consultations under "Public policy considerations for OTT" which garnered the most number of contributions, as well as a physical meeting held on 18 September 2017.

The outcomes of the events prove that there is a considerable interest in this direction in a plenty of countries. This is the reason we present some of the examples of OTT services regulation as the basis for experience exchange, as well as constructive discussion within CWG-Internet leading to recommendations to be approved, if necessary, to initiate the establishment of the international regulation.

1. **Proposals**

Russian Administration would like to support the studies conducted by ITU-T on technical, economical, regulatory aspects related to OTT, as well as the work performed by ITU-D, focused on assisting the developing countries. Russian Administration looks forward to finishing the existing studies and adopting the relevant ITU-T Guidelines.

We propose to arrange the discussion of issues related to OTT regulation at the national and international levels within CWG-Internet under the following general plan:

1. To invite state representatives to submit best practices of OTT legislation regulation.
2. To request ITU-D SG1, ITU-T SG3 and SG17 to submit to CWG-Internet their considerations on the issues related to OTT services requiring regulation.
3. To arrange within CWG-Internet a wide discussion with Member States participation and develop, if appropriate, recommendations for ITU Council on the role the states in OTT services regulation issues at the international level.

**Annex**

**Examples of regulatory practices for OTT services**

**as of 20.12.2018**

**1. RUSSIAN FEDERATION**

The practice of OTT services regulation is beginning to emerge in the Russian Federation. Nowadays providers under their business models are not required to mandatory authenticate the users, moreover there are no mandatory requirements and the international police in place. This situation gives rise to various kinds of conflicts in legal approaches, for example, for identical messaging services (voice/messaging) in circuit-switched networks there are requirements for security and client protection and in packet-switching networks - no.

In this regard, OTT messaging services can widely and easily used for unlawful, antisocial activities. In addition to OTT messaging services content services with user generated content pose a certain threat, getting exploited by terrorist, antisocial organizations for promoting their agenda that provoke users (mainly minors). Lack of regulatory mechanisms lead to a legislation vacuum.

OTT service providers are also interested in transparent, unified and uniform policies of user authentication and regulation. Today providers use their own judgment regarding unlawful user actions and take measures to identify the unlawful actions and criminal content, however, such efforts differ from provider to provider and are inefficient due to the cross-border nature of OTT services.

With respect to mentioned above, the Russian Federation prepared a national regulation – the Federal law No. 241-FZ "On amending Article 10-1 and 15-4 of the Federal Law "On Information, Information Technologies and Information Protection"[[1]](#footnote-1), which would make it mandatory for the messaging and OTT content providers (with respect to user generated content) to identify users via mobile subscriber number (MSISDN). Besides, the OTT provider is required to conclude the contract on identification between the instant messenger and communication operator and take user authentication in cases prescribed by the local laws, but nothing else.

Along with the identification obligations it is proposed that OTT service providers shall be responsible to implement technical feasibility for users to reject electronic messages from other users, to implement the means to receive e-messages sent under the discretion of public authorities (in emergencies) as well as to restrict the reception of messages containing information violating the local laws, through the decision of the responsible authorities.

**2. EUROPEAN UNION (EU)**

European Union regulates the activities of OTT providers using an array of laws and law initiatives. Both industry and horizontal regulation are present [[2]](#footnote-2). In particular, EU adopted in 2002 and supplemented in 2009 the so-called Telecoms package that contains 7 initiatives:

**1) Electronic Communications Framework Directive[[3]](#footnote-3)**

It is the principal regulatory document regarding the work of electronic communications networks and services in EU as a whole and in part of ensuring the user principal rights. The Directive authorizes the application of regulatory measures to OTT service providers:

*(7) "The provisions of this Directive and the Specific Directives are without prejudice to the possibility for each Member State to take the necessary measures to ensure the protection of its essential security interests, to safeguard public policy and public security, and to permit the investigation, detection and prosecution of criminal offences, including the establishment by national regulatory authorities of specific and proportional obligations applicable to providers of electronic communications services.".*

Furthermore, the right to a free reception/distribution of information, as well as the absence of censorship, is recognized:

*(6) "Audiovisual policy and content regulation are undertaken in pursuit of general interest objectives, such as freedom of expression, media pluralism, impartiality, cultural and linguistic diversity, social inclusion, consumer protection and the protection of minors.".*

**2) Directive on the authorisation of electronic communications networks and services (Authorisation Directive)[[4]](#footnote-4)**

The Directive is intended to issue authorisations to networks and electronic communications services, regardless of whether they are made public or not.

The goal of the Directive is to harmonize the market for electronic communications services by limiting regulation to the minimum necessary.

In the EU, OTT service providers located at least in one EU Member State have the right to provide communication services in all other EU Member States, without the need to have an office there. They can begin to provide communication services without any formal licensing process with the national regulator and are only subject to "general authorization" in each Member State where they provide services (see Article 3 of the Authorisation Directive). "General Authorisation" provides rights and imposes obligations on the use of networks and communication services by simply notifying the regulators, that reduces the licensing procedure just to a simple notification of the regulator.

**3) Directive on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)[[5]](#footnote-5)**

The Directive harmonizes access to electronic communications networks and related facilities in EU countries. It establishes a regulatory framework for relationships between providers of networks and communications services, that leads to a sustainable competition and interoperability of electronic communications services.

The Directive applies to all forms of public communications networks that provide public electronic communications services. These include fixed and mobile networks, networks used for terrestrial broadcasting, cable television networks, and satellite and Internet networks used for delivery of voice, fax, data and images.

The Directive establishes the fundamental rule that operators of public telecommunication networks are required to agree on interconnection with each other to ensure compatibility between services throughout the European Union.

National regulators are responsible for regular market analysis in order to determine whether one or more operators have a significant market power in the market in question (monopolists). If after market analysis, an operator is defined as having significant market power in a given market, the regulator must impose one or more of the following obligations on it, depending on the circumstances (transparency, elimination of discrimination, accounting separation, cost recovery and price control, etc.)

**4) Directive on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)[[6]](#footnote-6)**

Universal service is a concept developed by the European Union on a set of common interests that should be met by services such as telecommunications and postal services throughout the EU. The goal of the concept is to provide all users with the access to quality services at an affordable price regardless of their geographical location.

The Universal Service Directive establishes specific rules for the provision of electronic communications services within the EU. In this context it establishes:

• obligations to provide certain mandatory services (universal service);

• end-user rights and corresponding obligations in relation to companies that provide public networks and electronic communications services.

The Directive also provides:

• a consumer the right to change the fixed or mobile operator within one business day while maintaining his old phone number;

• an obligation for operators to provide transparent and timely information on prices and tariffs;

• free delivery of the European emergency number "112" with the requirement for operators to transmit information to the emergency services on the location of the caller;

• promotion of "116" numbers for social services, including "missing children" emergency phone number.

**5) Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive)[[7]](#footnote-7)**

*REPLACED*

The Directive applies to the harmonization of national provisions necessary to ensure an equivalent level of protection of the fundamental rights and freedoms of both individuals and legal entities in electronic communications. In particular, the rights to privacy, confidentiality of personal correspondence and the protection of personal data in the electronic communications sector. It guarantees free circulation of data, equipment and services in the EU.

On May 25, 2018, the Directive was cancelled due to its replacement by the Regulation on Privacy and Electronic Communications.

**Regulation on Privacy and Electronic Communications[[8]](#footnote-8)**

The Regulation pursues objectives similar to those of the replaced Directive 2002/58/EC. The EU Council holds monthly hearings on the need for any changes.

**6) Regulation (EC) No 1211/2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office)[[9]](#footnote-9)**

By adopting this Regulation, the Body of European Regulators (BEREC) was established, which advises EU institutions on creating the best market for electronic communications networks and services and organizes communication between national regulators and the European Commission, disseminating best practices among regulators.

**7) Regulation (EU) No 531/2012 on roaming on public mobile communications networks)[[10]](#footnote-10) (amended on May 17, 2017)[[11]](#footnote-11)**

From July 1, 2012, the Regulation eliminated roaming charges when travelling within the EU. This means that EU citizens travelling within the EU can make calls, send text messages and have access to the Internet on their mobile devices at the same price as in their own countries.

The Regulation also sets out security measures for protecting mobile operators from abuse, and operators could maintain new roaming rules without raising domestic prices.

The following EU-adopted initiatives are complementary for the OTT industry:

**Audiovisual Media Services Directive[[12]](#footnote-12)**

The Directive aims to create a framework for cross-border audiovisual media services in order to strengthen the domestic market for production and distribution of programs and ensure fair competition.

The Directive establishes legal, regulatory and administrative provisions related to the provision and distribution of audiovisual media services.

EU countries shall not limit rebroadcasting of audio-visual media services from other EU countries on their territories until broadcasting programmes do not become violent or pornographic, capable of hurting the feelings of minors.

EU countries may also limit the content delivery on the territory if a national regulator is suspicious about the state policy, security or consumer protection may be at risk. In particular, in 2014 in France and Spain ОТТ services providers operating by connection to the public switched telephone network (PSTN) were prohibited to provide voice services. This prohibition was justified by the fact that ОТТ acted like a fully functional carrier company, but did not fulfil the obligations of a traditional telecommunication company (did not pay for universal communications services according to the legal requirements, did not provide the ability to call Emergency Services, disclaimed liability for the breach of national legislation). [[13]](#footnote-13)

Audiovisual services provider shall disclose the following information to the consumer:

- its name;

- its geographical address;

- its contact details;

- relevant regulating or supervisory authorities.

When providing on-demand audiovisual information services (Video On Demand), EU countries shall ensure required conditions for providers of audiovisual media services so that they facilitate the production of and access to European content. With this purpose providers may make financial contributions to the production of European content or they may reserve a share and/or increase popularity of European content in their program catalogues.

AVMS Directive (Audiovisual Media Services) was amended and adopted on 6 November 2018.

New additions:

• Several rules of the revised Directive are now extended to cover video sharing platforms such as: YouTube as well as audiovisual content distributed in social networks such as Facebook.

• Increased protection of minors from harmful content in digital world is provided: new rules increase the safety of "video on demand" services with the commitment to protect the minors also being extended to video sharing platforms which now must take appropriate actions.

• Protection of TV and video on demand services from violence/hate rhetoric and public incitement to conduct terrorist crimes has been increased. Platforms for video sharing must also take appropriate measures to protect people from violence/hate rhetoric as well as from the content constituting criminal offences.

• Increased commitment to promote European audiovisual titles for VOD services which are required to have at least 30% of European content in their catalogues and ensure that this content is sufficiently covered.

• Reinforced provisions on protection of children from inappropriate audiovisual commercial messages for the products with high fat, salt and sodium, and sugars content including by promoting codes of conduct at the EU level, where appropriate. Video sharing platforms should also comply with specific obligations with respect to commercial messages, for which they are responsible, providing transparency of these messages placed on user uploaded content.

However, the legal and regulatory framework given above does not fully comply with the tasks of efficient protection of personal data (PD) on the Internet, in general, and in ОТТ services, in particular. For that reason, in recent years EU has developed more detailed legislative framework in this area which would cover all EU countries as well as partially third countries, taking into account changes in existing EU system for processing personal data of customers. The legislative framework developed is called **"Personal data protection legislative package"[[14]](#footnote-14)** which includes two documents, intended to replace obsolete legal framework:

1) "General Data Protection Regulation" (GDPR),

2) "Directive (EU) – protecting individuals with regard to the processing of their personal data by police and criminal justice authorities".

**1) EU General Data Protection Regulation 2016/679)[[15]](#footnote-15)**

EU General Data Protection Regulation 2016/679 is the EU regulation adopted by the European Parliament on 24 May 2016 according to the results of lengthy discussions. It entered into force on 25 May 2018. The adopted document in the field of PD protection has the status of regulation, in contrast to the prior directive.[[16]](#footnote-16) This regulation has replaced Directive 95/46/EC which was prior in force, better known as EU Directive on protection of natural persons with regard to the processing of personal data.

It allows European Union citizens to better control their personal data. It also updates and unifies rules allowing enterprises to reduce bureaucracy and enjoy greater consumer confidence.

As compared to the obsolete Directive 95/46/ЕС, new regulation strengthens already existing citizen rights providing them with new ones as well as granting the citizens more control over their PD. In particular, these include:

• Increased rights of PD subjects. The regulation specifies and expands the rights of citizens as subjects of PD. Thus, PD subjects have the rights to:

1. receive the proof of the fact of PD processing;
2. demand furnishing copies of such PDs;
3. demand providing additional information (stating the purpose for processing, PD categories, recipients, dates etc.);
4. protest against PD processing for specific purposes;
5. demand full removal of PD or temporal restriction of the use of such PD,

• More transparent "Right to Be Forgotten",

• New right to transfer data among services providers,

• New right to know that PD of a citizen were hacked/compromised. Organizations are obliged to disclose information on occurred hacks or PD compromising. Organizations, supervising PD, must notify the regulator on such cases as well as PD subjects themselves, under specific conditions.

In addition to PD subjects, the regulation is applied not only to PD processing organization which have been established on the EU territory, but to other organizations which work directly on the European market. All online services offering services in different languages and accepting Euro as payment, as well as data centers located on the territory of third-party states and collecting PD of Europeans (Dropbox, Mega, iCloud etc.) could be considered as most likely "victims" among such organizations.

**2) Directive (EU) on the protection of natural persons with regard to the processing of their personal data by police and criminal justice authorities (Data Protection Directive 2016/680 for Police and Criminal Justice Authorities)[[17]](#footnote-17)**

On an equal footing with an obsolete Framework Decision 2008/977/JHA (see below), this Directive is intended to protect natural persons’ personal data when processed in the police and criminal justice authorities, and provides more effective information exchange required for conducting investigation activities. The data collected are protected from unauthorized or illegal processing. EU Members States have implemented this Directive in accordance with their national laws (harmonization) and it entered into force on 6 May 2018.

**The Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Council Framework Decision 2008/977/JHA of 27 November 2008)[[18]](#footnote-18)**

*REPLACED*

It is intended for the protection of fundamental rights and freedoms of people, when their personal data are processed for the purpose of preventing and combating crime, facilitating investigation, criminal prosecution and criminal punishment. In particular, the timeframe for the work with personal data of citizens for the purpose of processing, transfer, as well as rights of subjects of this data and their protection by relevant authorities is established.

This document was replaced by the EU Directive 2016/680 (see above) which entered into force on 6 May 2018.

**Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data[[19]](#footnote-19)**

*REPLACED BY GDPR*

The Directive specifies the regulatory framework aimed at achieving a balance between high level of privacy protection and free circulation of PD within the EU. For this purpose the Directive establishes strict restrictions on PD collection and use and requires that each Member State creates an independent national authority responsible for the control over any activity related to PD processing.

The Directive is applied to both data processed by automated tools (for example, computerized customer database), and data contained or intended for use in unautomated workflow systems (traditional paper documents). The transfer of PD from a Member State to a third party with an adequate protection level is permitted.

**E-Commerce Directive (Directive on privacy and electronic communications) [[20]](#footnote-20)**

This EU Directive regulates different matters related to online commerce in "information society services", such as, among others, ОТТ services.

The Directive establishes the principle, according to which service operators (including ОТТ) are subject to regulation related to service providing/search, only in a EU country, where they have a registered headquarters, and not in a country where servers, e-mail addresses or mail boxes used by them are located.

National EU governments ensure the publication by the operators of the basic information on their activities (name, address, commercial register number etc.) in easily accessible way.

Regulation relates to the following services to be provided:

- News services (news sites);

- Sale (books, financial services, tourist services etc.);

- Advertisement;

- Professional services (lawyers, physicians, real-estate agents);

- Entertainment services;

- Basic intermediary services (access to the Internet, transfer and posting of the information);

- Free services, financed by advertising, sponsorship etc.

Unsolicited e-mails ("spam") should be clearly identified. Companies sending spam e-mails must regularly check with and consult with "reject mail lists" which may include people unwilling to receive spam e-mails.

**Principles and guidelines for the audiovisual policy (Principles and guidelines for the Community’s audiovisual policy in the digital age)[[21]](#footnote-21)**

ABOLISHED

The Directive on principals and guidelines for the audiovisual policy in the digital age (remains in force but is obsolete).

**3. USA**

In USA ОТТ providers are not required to have licenses to provide communications services, however there are some obligations in terms of providing emergency calls as well as responsibility for violating USA legislation.

In 2015 the USA regulator, the Federal Communication Commission (FCC) formalized strict rules with regard to network neutrality – Open Internet Order.

Since 2011, the White House and the Federal Trade Commission (FTC) have issued several important documents. Although in these proposals no particular emphasis has been placed on OTT services, they aim to protect personal data used in obtaining services on the Internet.

**Safe Harbor**

*REPLACED*

A special agreement between the United States and EU (Safe Harbor) – is a system of self-regulation with some regulatory principles whereby the companies in the United States sign Principles of confidentiality and complaints system. The aim of the agreement is to assure business enterprises that by giving PD to partner states within Safe Harbor in USA, all their confidential personal data transferred outside the EU, will be properly protected. The system is supervised by the Federal Trade Commission. As of 6 October 2015 the concept was considered invalid. Privacy Shield was proposed to implement the transatlantic exchange of personal data for commercial purposes complying with all the data protection requirements of the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on free movement of such data.

**Privacy Shield**

The EU-US Privacy Shield reflects the requirements set out by the European Court of Justice in its ruling on 6 October 2015, which declared the old Safe Harbor framework invalid. Since 1 August 2016 the new arrangement will provide stronger obligations for companies in the US to protect the personal data of the European citizens and stronger monitoring and enforcement by the US Department of Commerce and Federal Trade Commission (FTC), including through increased cooperation with European data protection authorities. The new agreement includes obligations by the US state bodies to avoid disclosure of the personal data. In this regard, Europeans will have the possibility to raise any enquiry or complaint in this context with a dedicated new Ombudsperson[[22]](#footnote-22).

In the annual Report No. 13-99 of the Federal Communications Commission (FCC) on status of video content delivery the notion of "Online Video Distributor (OVD)" is introduced and is defined as "any entity that offers video content by means of the Internet or other Internet Protocol (IP)-based transmission path provided by a person or entity other than the OVD"[[23]](#footnote-23).

The following professionally produced content can be distinguished:

(1) semi-professionally produced video that relates to the consumer or user content with professional or production qualities (for instance, video filmed with professional equipment using professional skills), as well as content produced solely for online audiences; and

(2) user-generated content that is publicly available, created by end users, often with little to no brand equity or brand recognition.

As of 2018 more than 4,000 companies are certified (comply with the provisions) by Privacy Shield.

**4. BRAZIL**

Telecommunications services are regulated and monitored by ANATEL – the agency that is responsible for implementing national telecommunications policy and for carrying out most of the administrative activities associated with telecommunications providers. In 2015 the telecommunication operator "Telefônica Brasil" called the WhatsApp administration "pirates" due to the threat WhatsApp poses to the traditional SMS messaging and sent a request to ANATEL to develop and approve the regulation for OTT services.

Marco Civil da Internet (Law No. 12.965) – is the current law, known as the "Brazilian Civil Rights Framework for the Internet", which regulates the use of the Internet in Brazil by regulating the guarantee principles, rights and obligations for using the Internet, as well as defines the guidelines for the state.

OTT service providers have to provide ANATEL with information that allows them to verify compliance with Brazilian legislation in part of collecting, compiling, storing and using data, as well in part of complying with data and communications confidentiality requirements.

The law is aimed at protecting PD of Internet users and ensuring the principles of network neutrality. It also limits the categories of user data that Internet service providers can store and collect.

The provisions cover records of committed communication instances (calls) and information about access to applications that cannot be transferred to third parties without the voluntary, explicit and informed consent from an individual. The content of private communications can only be disclosed by a court decision, in situations and according to procedures defined by law.

The law establishes net neutrality: "Any traffic discrimination or deterioration of quality of services that do not count as necessary technical requirements for the adequate provision of services are prohibited". Providers are required to transfer data on an equal basis, regardless of the content of this data, their source and destination.

It is also forbidden in the process of providing both paid and free access to the Internet, as well as when transmitting, switching and routing, to block, monitor, filter or analyze the data packet content.

**5. INDIA**

In 2015 the Telecom Regulatory Authority of India (TRAI) formed a Net Neutrality Committee

In March 2015 TRAI issued the official consultation paper on developed Regulatory Framework for OTT services. This consultation paper was discussed by Indian Internet users.

On 8 February 2016 TRAI decided to prevent telecom service providers from offering differential pricing plans based on content, thereby establishing Net Neutrality in India.

In May 2016 a study on interaction between the incumbent network providers and OTT providers was released. The operators were forbidden by TRAI to provide communication services to end-users free of charge in accordance with "Prohibition of Discriminatory Tariffs for Data Services Regulations". This was justified by Net Neutrality Framework, which prohibited differential prices for data services that would restrict access for the end users.

**6. REPUBLIC OF SOUTH AFRICA**

In an effort to create equal conditions for all operators, currently traditional South African telecom operators are seeking regulatory intervention from the government of the country, since OTT services in South Africa are not licensed, do not have tax obligations, and do not provide security for the national infrastructure. South Africa's main operators (Vodacom and MTN), as well as a small operator (Telkom Mobile), lead a jointly public campaign for the government to address a number of issues pertaining to OTT services.

A number of African operators have preferred to use OTT services to protect and increase their market share. Such operators offer consumers to use data transfer services for free, or through combining dedicated data streams for social media services, or by using the Free Basics app provided by Internet.org.

1. <http://www.kremlin.ru/acts/bank/42199> [↑](#footnote-ref-1)
2. Over-the-Top players: market dynamics and policy challenges // <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf> [↑](#footnote-ref-2)
3. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0021-20091219> [↑](#footnote-ref-3)
4. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l24164> [↑](#footnote-ref-4)
5. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0019> [↑](#footnote-ref-5)
6. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1545309184652&uri=CELEX:32002L0022 [↑](#footnote-ref-6)
7. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010 [↑](#footnote-ref-7)
8. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010 [↑](#footnote-ref-8)
9. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:si0015> [↑](#footnote-ref-9)
10. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32017R0920> [↑](#footnote-ref-10)
11. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32017R0920> [↑](#footnote-ref-11)
12. <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0013> [↑](#footnote-ref-12)
13. The rise of OTT players – what is the appropriate regulatory response? Detecon Consulting // <https://www.detecon.com/sites/default/files/Paper_OTT_Player.pdf> [↑](#footnote-ref-13)
14. <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> [↑](#footnote-ref-14)
15. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG> [↑](#footnote-ref-15)
16. Principal characteristic is that EU regulations once approved become directly enforceable over the whole territory of EU Member States, while directives are introduced through national legislation of each European state. [↑](#footnote-ref-16)
17. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680> [↑](#footnote-ref-17)
18. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008F0977> [↑](#footnote-ref-18)
19. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046> [↑](#footnote-ref-19)
20. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32000L0031> [↑](#footnote-ref-20)
21. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l24223> [↑](#footnote-ref-21)
22. EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield // <http://europa.eu/rapid/press-release_IP-16-216_en.htm> [↑](#footnote-ref-22)
23. <https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-99A1.pdf> [↑](#footnote-ref-23)