# THE UDRP: A BRAND PROTECTION TOOL IN THE POST-GDPR WORLD

Imge Gören
ANR 625127, SNR 2031414

Master's Thesis
LLM Law & Technology
Tilburg Law School
Tilburg University, Tilburg

First Reader: Martin Husovec, PhD
Second Reader: J. P. Waterson
May 2019
Words 16,937

## List of abbreviations

| | |
|---|---|
| **ADR** | Alternative Dispute Resolution |
| **ccTLD** | Country Code Top-Level Domain |
| **CJEU** | Court of Justice of the European Union |
| **DPIA** | Data Protection Impact Assessment |
| **DPO** | Data Protection Officer |
| **EDPB** | European Data Protection Board |
| **GDPR** | General Data Protection Regulation |
| **GNSO** | Generic Name Supporting Organization |
| **gTLD** | Generic Top-Level Domain |
| **ECHR** | European Convention on Human Rights |
| **ECtHR** | European Court of Human Rights |
| **EURid** | European Registry for Internet Domains |
| **ICANN** | Internet Cooperation For Assigned Names and Numbers |
| **INTA** | International Trademark Association |
| **IP** | Intellectual Property |
| **IP** | Internet Protocol |
| **IPO** | Intellectual Property Office |
| **IPR** | Intellectual Property Rights |
| **RAA** | Registrar Accreditation Agreement |
| **TLD** | Top-Level Domain |
| **UDRP** | Uniform Domain-Name Dispute Resolution Policy |
| **WIPO** | World Intellectual Property Office |

# Table of Contents

# Chapter 1. Introduction

The technological development around the world accelerates the globalisation and the speed of globalisation pushes lawmakers to find new cross-border solutions. In this context, intellectual property (IP) is one of the most affected fields of law due to its uniform structure that requires international regulations.

Nowadays there have been steps to make the IP system uniform by regulating international organizations, offices and some alternative dispute resolutions outside the court. Arbitration is the best way to catch up with the rapid changes in technology.[1] Arbitration has more distinct advantages compared to litigation in local courts, such as low-cost and time-sensitive procedures. In addition to this, the lack of an expert decision maker in litigation is the main reason why arbitration is better suited to resolve complex technical or scientific disputes.[2] Nowadays, due to the merging of internet connectivity and the General Data Protection Regulation (GDPR), another feature of arbitration becomes more prominent, which is flexibility. This will be the subject to review in Chapter 2.

Taking into the consideration the advantages of arbitration, it may be said that arbitration is going to be the most suited dispute resolution system in the field of IP. WIPO has already one global leader alternative dispute resolution system, namely the Uniform Domain Name Dispute Resolution Policy (UDRP). This dispute resolution system will be the pioneer and inspiration in executing other alternative dispute resolution systems related to IP. In light of this information, the importance of the UDRP will be analysed in Chapter 2.

In order to explain how this alternative dispute resolution works, we need to know some definitions. First of all, the UDRP is one of the most important processes which was adopted by Internet Corporation for Assigned Names and Numbers (ICANN) in 1999. The ICANN is a private, non-profit organization located in the USA. This organization is responsible for many important duties such as domain name system management, IP address space allocation and root server system management. [3] ICANN has a very strong and close cooperation with the WIPO. In a nutshell, UDRP is a policy regulated by ICANN, which was operated by WIPO.

When a domain name is being bought, the registrant has to accept the policy of ICANN, which includes the UDRP process. When a registered trademark owner detects an infringement, the owner may lodge a complaint before WIPO to transfer the disputed domain or cancel it. The success of the complaint depends on the existence of three elements of the UDRP. Basically, pursuant to Article 4(a) of the Uniform Domain-

[1] Maud Piers, Christian Aschauer, *Arbitration in the Digital Age: The Brave New World of Arbitration*, Cambridge University Press, Cambridge, 25 Jan 2018.
[2] Raymond G. Bender, Arbitration—An Ideal Way to Resolve High-Tech Industry Disputes, *The Dispute resolution Journal* November 2010 / January 2011, Vol.65, No. 4 pp. 1- 9.
< https://svamc.org/wp-content/uploads/2015/08/Arbitration-An-Ideal-Way-to-Resolve-High-Tech-Industry-Disputes.pdf> (consulted in 12 December 2018)
[3] https://www.icann.org/resources/pages/what-2012-02-25-en

Name Dispute-Resolution Policy (hereinafter UDRP policy), the Complainant has to prove the presence of the following three provisions: (i) the conflicted domain names are the same with or similar enough to cause confusion with the Complainant's trademark; and (ii) the Complainant has no right or legitimate interest on the conflicted domain names of the respondent; and (iii) the conflicted domain names were registered and are used in bad faith by the respondent. This alternative dispute resolution system has been accepted by many countries in the world. While some countries have accepted UDRP only for Generic top-level domains (gTLDs, for instance .com, .gov, .edu, .net) some of them have accepted it also for country code top-level domain (ccTLD, for instance .nl, .ru, .ca, .uk, .eu)[4].

In 2018, the system faces some challenges due to the fact that the General Data Protection Regulation (GDPR) came into force. In parallel with the EU, data protection legislations also came into force in other countries that adopt the UDRP policy for their country code top-level domains. In other words, data protection policies pose a challenge not only in the EU but also in the countries where data protection law is adopted.

In general, it can be said that the GDPR has two articles that undermine the UDRP. Firstly Article 5/1of GDPR requires that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes. Secondly, Article 5/3 requires that personal data shall be collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In a nutshell, UDRP lacks legitimate purposes in collecting the data and if the data is collected, it may be infringement of data minimisation principle mentioned in Article 5 (3).

Does the WHOIS database[5] not have a legitimate purpose which is providing information to trademark owners to protect their property in collecting personal data such as the name and address of domain holders? Taking into consideration the disadvantages of full anonymity in the internet, it may be accepted that it has legitimate purposes. On the other hand, before the GDPR, hosting companies could offer their domain privacy service such as a proxy and privacy service to their customers. When there is a complaint, the whole information will be made invisible to the third parties such as trademark attorneys, legal counsels. Actually, the UDPR was possible without the full details of the domain registration before the GDPR, thus, legitimate interest in collecting data will not appear so realistic in the current situation. Under these circumstances, registrar companies reject to share his personal data to ICANN for WHOIS. This will be analysed in Chapter 4.

[4] This link shows the participation of ccTLD agreements according to countries, <http://www.wipo.int/amc/en/domains/cctld_db/output.html> (consulted in 12 December 2018)

[5] WHOIS is a sort of research engine which shows the information about domain name registration details including personal data of domain name owners. <https://whois.icann.org/en/basics-whois> (Consulting in 14 May 2019)

In the absence of legitimate interest and the necessity of collecting personal data, hosting companies have started to change their requirement in order to comply with GDPR. For instance, GoDaddy, which is one of the biggest domain registrars and hosting companies, has announced that if a domain name contains contact information of an individual in the European Economic Area (EEA), a WHOIS search will return only domain technical information, Registrant Country and State/Province. The rest of the contact information will be removed from the results.[6] Registrant ID, registrant email (Anonymized email or web form), registrant name, registrant street, city, country and postal code, admin organization, admin street, city, state, country, postal code, admin phone ext., admin phone, admin fax, admin mail, registry tech ID, tech name, tech organization, tech city, tech country, tech phone fax, Tech Fax Ext, tech mail (Anonymized email or web form) are not displayed on WHOIS after the GDPR[7].

Why is the information on WHOIS very important? WHOIS allows free public access to personal information such as the name of the domain owner and address. Every owner of a trademark has the chance to know the owner of the domain names via the WHOIS database. They can contact and negotiate to transfer or cancel the disputed domain. After learning the identity of the domain name owner, the owner of the trademark may research in which field that domain will be used by monitoring the trade registry offices. It may be researched whether the owner of the domain has a trademark registration or application. Consequently, it is clear that the WHOIS database provides an opportunity of preliminary examination to the trademark owner. In this way, the trademark owner may predict the chance of success in a UDRP complaint before the WIPO arbitration centre.

There is no denying of the fact that the approaches of the panel of WIPO in post- GDPR world need to be changed in order to overcome the challenges that the GDPR brings forth. Which aspects should be evaluated by arbiters in more flexible perspectives is explained in Chapter 3. It is needed to adopt a more flexible approach, since there is not enough clarification on how the complainant will prove the respondent`s bad faith. In addition to this it is not clear how we can be sure that the respondent has no legitimate interest in holding or using the disputed domain without any data of owners of domain names. It is also expected that blanket judicial discretion will be given to panels or arbiters. Furthermore, another issue may be that it was possible to file a complaint for multiple domains registered to the same owner before the GDRP. In this sense, it is still unknown how the UDRP will be integrated.

The first case related to the problems that the GDPR caused was lodged in Germany. EPAG, a German-based domain registrar informed ICANN that they are not going to collect personal information when registering a domain name. They referred to the GDPR as its justification. ICANN filed suit in Germany seeking an injunction to force

[6] The Announcement of Godaddy regarding the collecting <https://in.godaddy.com/help/why-is-domains-by-proxy-no-longer-available-in-gdpr-affected-areas-27925> (consulted in 5 November 2018)
[7] General Data Protection Regulation (GDPR) & WHOIS at ICANN, ICANN, Savenaca Vocea APNIC 46, Noumea 11.09.2018 <https://conference.apnic.net/46/assets/files/APNC402/GDPR-and-Whois-at-ICANN.pdf> (Consulted in 3 November 2019)

EPAG to collect the contact information. However, ICANN`s lawsuit was rejected by the German courts, which is going to be deeply analysed in Chapter 4.

In line with these developments, It is clear that the UDRP may lose its efficiency and it may become obsolete, unless it can find a way for the future of WHOIS. Taking into the consideration the importance of the UDRP, It should be focused on how the UDRP may keep its sufficiency. At this point, WIPO has announced that if a UDRP complaint contains all available registrant information, the complaint would be accepted by WIPO for processing and compliance review. In addition to this, WIPO introduced `` Temporary Specification for gTLD Registration Data`` which proposed that users will also maintain the ability to contact the Registrant or Administrative and Technical contacts through an anonymized email or web form[8]. Moreover, third parties claimed a legitimate and proportionate purpose will be able to access the non- public WHOIS database. In order to GDRP compliance, ICANN's Temporary Specification regulates WHOIS requires registry operators and registrars to grant access to non-public WHOIS information on the basis of legitimate interests pursued by the requesting party.[9] In this respect, in Chapter 4, the ideas of ICANN and WIPO will be discussed.

Consequently, we will conclude this thesis in the light of the research question that is ``what are the impacts of the GDPR on the process of the UDRP and what steps can be taken by ICANN to keep the efficiency of the UDRP?``

[8] Temporary Specification for gTLD Registration Data, Annex: Important Issues for Further Community Action. More details in the Section 2.5.1 of Appendix A, ICANN, 2018 <https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#appendixA> (Consulted in 5 November 2018)

[9] WHOIS Challenges: A Toolkit for Intellectual Property Professionals, INTA, 2015 <https://www.inta.org/Advocacy/Documents/2018/WHOIS%20Challenges%20A%20Toolkit%20for%20Intellectual%20Property%20Professionals.pdf> (consulted by 5 November 2018)

# Chapter 2. The Importance of the UDRP in The Era Of the Internet

## 2.1. The Place of the UDPR in Arbitration

Arbitration has become the most traditional and well-known form of alternative dispute resolution in parallel with the spreading usage of internet and technology in many fields. It is important to emphasises that the UDRP is not theoretically an arbitration system. It has an unique legal conflict resolution system that was created by ICANN to tackle cybersquatting.[10] The UDRP can be accepted as a mandatory administrative proceeding, since ICANN requires domain name registrars to agree on a clause stating that the registrant agrees that all claims involving cybersquatting or bad faith registration will be resolved with the UDRP.[11] However, in this thesis, the focus will be on the necessity and the need of the resolutions systems in the era of technology rather than focusing on the technical differences between the UDRP and the arbitration. Herein the UDRP has been accepted as a type of arbitration.

The rapid increase of technology forces the system and lawmakers to think and create more effective dispute resolution systems, which makes us rethink about our principles and leading cases in our own legal system. For instance, the principle of territoriality in intellectual property rights has been undermined in the protection of IP rights, since the borders are getting blurred in the era of the internet. Prevention of violations of patents, copyrights or trademarks protected in various countries may require the filing cases in multiple foreign courts, including judges with different jurisdiction and many degrees of experience and expertise.[12] Moreover, it should not be forgotten that there is always a risk which is that the court decisions may conflict with each other, since interpretation of an infringement may differ according to jurisdictions. Even if an IP rights holder takes legal action and becomes successful, IPRs may face some difficulties in enforcement due to the lack of an international treaty or long process of the recognition and enforcement.[13]

Taking into consideration the risk of inconsistency in national approaches, the untrusted legal system in many countries and the unexpected expense of enforcing foreign judgments, it should be accepted that arbitration offers more effective solutions compared to litigation[14]. Especially, in intellectual property disputes, there are many particular characteristics of arbitration that may be better addressed by arbitration than

[10] Elizabeth C. Woodard, The UDRP, ADR, and Arbitration: Using Proven Solutions to Address Perceived Problems with the UDRP, *Fordham Intellectual Property, Media and Entertainment Law Journal*, 2009, Vol 19, No 4, pp 1170-1212.
[11] Id., p. 1193.
[12] Joseph P. Zammit and Jamie Hu, Arbitrating International Intellectual Property Disputes, *Dispute Resolution Journal*, November 2009/ January 2010, pp 1-4.
[13] Id., p. 2.
[14] Arbitration as A Dispute-Solving Mechanism in Public Procurement: A Comparate View Between Peruvian and Spanish Systems, Alexandra Molina Dimitrijevich,<http://www.ippa.org/IPPC4/Proceedings/01ComparativeProcurement/Paper1-18.pdf> (Consulted in 15 November 2019)

by court litigation. These characteristic advantages of arbitration are flexibility[15], neutrality[16], enforceability[17], confidentiality[18].

The UDRP with the abovementioned features has an important effect in struggling with counterfeiting. Particularly, the UDRP may also be a better solution in combating with counterfeiting especially for non-deceptive counterfeiting that will be explained in the next section.

### 2.1.1. The Effect of Internet on Counterfeiting

Regarding dealing with counterfeiting and piracy, there are multiple ways such as consumer education, physical control and restrictions, market surveillance and most importantly monitoring trademarks and enforcing IP rights. On top of that rights holders and law enforcement authorities need to have proper legal tools to enforce these underlying trademark and related laws. At this point, taking into account the difficulties of cross-board legal actions, arbitration should be a key in dealing with the piracy in an effective way. Since, criminals have vast and major opportunities to engage in online trade of counterfeit goods due to the continuous growth of the internet. The criminals employ international operating methods which increases the challenges for cross-border investigations by law enforcement and this often hampers prosecutions in multiple jurisdictions.[19]

Given the rising problem of the infringement on the internet[20], arbitration offers a solution by considering the party that sells or uses counterfeit products is in bad faith. For instance, in the Administrative Panel Decision of the WIPO Arbitration and Mediation Center, namely Bayerische Motoren Werke AG (BMW) v. Balog Sebastian[21], the panel notes that the Respondent has used the disputed domain names to offer counterfeit, illegitimate goods (software) under the BMW mark, and that subsequently, after the complainant complained to PayPal about the respondent's illegal use, the respondent suspended such offerings and replaced one of them by third party goods (ladies' sportswear). The participant intentionally tries to attract internet users to the websites or other online locations, creating the possibility of confusion with the BMW brand of complaint for commercial gain by using the controversial domain

[15] Cheryl H. Agris, Stephen P. Gilbert, Charles E. Miller and Sherman Kahn, The Benefits of Mediation and Arbitration for Dispute Resolution in Intellectual Property Law, *New York Dispute Resolution Lawyer*, 2011, Vol. 4 No. 2 pp 61-65.
[16] Massoud, M. F., *International Arbitration and Judicial Politics in Authoritarian States Law Soc Inq*, 2014, vol 39, issue 1, pp 1-30.
[17] Andrew Bartlett, Ashley Morgan, Osborne Clarke, Enforcement of judgement and arbitral awards in the UK overview, *Enforcement of Judgements and Arbitral Awards in Commercial Matters Global Guide 2018*, 2018, pp 1-16.
[18] Bernardo M. Cremades & Rodrigo Cortes, The Principle of Confidentiality in Arbitration: A Necessary Crisis, *Journal of Arbitration Studies*, 2013, vol 23 No 3, page 25-38.
[19] 2017 Situation Report on Counterfeiting and Piracy in the European Union, A joint project between Europol and the European Union Intellectual Property Office, 2017 <https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union> (consulted in 5 December 2018)
[20] Internatinal Trademark Association, Addressing the Sale of Counterfeits on the Internet, INTA, 2017 <https://www.inta.org/Advocacy/Documents/2018/Addressing_the_Sale_of_Counterfeits_on_the_Internet_021518.pdf> (Consulted in 17 May 2019)
[21] WIPO Arbitration and Mediation Center, Panelist Roberto Bianch, Bayerische Motoren Werke AG (BMW) v. Balog Sebastian Case No. D2017-1407, Administrative Panel Decision, 18 September 2017.

names. In accordance with paragraph 4 (b) (iv) of the policy, this is a condition of the use of registration and malicious intent. In another decision of the WIPO, the infringement of copyright was also considered as a proof of bad faith. In the decision of Star Stable Entertainment AB v. Dawid Olszewski, the panel found that the use of the disputed domain name linked to a website which had the look and feel of the official website of the complainant and was using the complainant's copyright-protected images, which is evidence of bad faith registration and use.[22]

Even though the UDRP is the resolution system for trademark protection, it emphasizes the importance of whether the content of the website includes any other IP infringements apart from the trademark infringement. We see the reflection of the UDRP case law on a new model called DNA. The DNA[23] (domain name association) announced health domain initiative recommendations where a method of taking down domain names in the event of copyright infringement has been recommended. One of the most interesting suggestions is to create a model of copyright infringement that is designed on the basis of the UDRP. This new resolution system allows copyright owners to apply an expert panel when there is a copyright infringement in the website.[24]

### 2.1.2. The Effect of Developing Countries in Counterfeiting

According to the joint project of Europol and European Intellectual property office[25] and United States International Trade Commission[26], the most prominent country for IP infringement is China. Concerns over major technology, fashion, and content creating firms in the United States, in developed countries are currently and mainly focused on China. If the problem needs to specified, the main points can be digital piracy, trademark infringement, counterfeit goods production, and industrial espionage[27]. According to the report of the US Chamber of Commerce, namely measuring the magnitude of global counterfeiting: creation of a contemporary global measure of physical counterfeiting;

[22] WIPO Arbitration and Mediation Center, Star Stable Entertainment AB v. Dawid Olszewski, Administrative Panel Decision, 27 July 2018, Case No. D2018-1293

[23] ("The DNA") is a non-profit global business association that represents the interests of the domain name industry.
<https://thedna.org/what-is-the-domain-name-association/> (Consulted in 8 April 2019)

[24] DNA Healthy Domains Initiative Registry / Registrar Healthy Practices, Domain Name Association's (DNA) Healthy Domains Initiative (HDI), 2017
<https://domainnamewire.com/wp-content/Health-domains.pdf> (Consulted in 8 April 2019)

[25] 2017 Situation Report on Counterfeiting and Piracy in the European Union, Europol and the European Union Intellectual Property Office, 2017.
<https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union> (Consulted in 14 January 2019)

[26] China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy, United States International Trade Commission, 2011
<https://www.usitc.gov/publications/332/pub4226.pdf> (Consulted in 8 January 2019)

[27] Maskus, Keith, *Private Rights and Public Problems : The Global Economics of Intellectual Property in the 21st Century*, Peterson Institute press 2012, Washington DC, 2012.

> ` 72 % of counterfeit goods currently in circulation in three of the world's largest markets for such products, namely the EU, Japan and the USA, have been exported from China.`[28]

The counterfeiting can be analysed in two types, namely non-deceptive and deceptive. In deceptive counterfeit products, trademarks, logos and designs are copied to enable consumers to believe that they are buying the legitimate product.[29] Non-deceptive counterfeiting is a more complex issue that should be researched by the experts of behaviour science. In non- deceptive counterfeits, customers are aware that the products that they buy are fake. In developing countries, it is harder to deal with the counterfeit in practise. Since, firstly, the deceptive counterfeiting exists because of the lack of economic power of a public in a developing country, since local people cannot afford the original product. Typical example of this can be counterfeit drugs in India.[30] Secondly, when the matter is non-deceptive counterfeiting, producing a counterfeit product is more likely to be tolerated by officials in developing countries.[31] Moreover, customers in even developed countries order fake products on purpose online. The best example of it that we can see today is counterfeit product that are being sold on Instagram[32]. Since the social media is the platform where the UDPR does not provide a solution. Today the UDRP prevents to spread of the counterfeit sales over websites which would cause the sales of deceptive counterfeit products.

Regarding counterfeit, although scholars have given due attention to the policies of international IP agreements, they have so far not shown enough interest in the policies of their practice and the political aspects of IP reform in the developing countries.[33] The economy and political situations are generally very fragile in developing countries. Therefore, if their economy benefits from counterfeit products in short-term, it is hard to change the system, even though the truth is that the weak IP protection is harmful to their economy in long term.

---

[28] Measuring the magnitude of global counterfeiting: creation of a contemporary global measure of physical counterfeiting, US Chamber of Commerce, Washington DC, 2016. <https://www.uschamber.com/sites/default/files/documents/files/measuringthemagnitudeofglobalcounterfeiting.pdf> (Consulted in 9 January 2019)

[29] The Economic Effects of Counterfeiting and Piracy, A Review and Implications for Developing Countries, Policy Research Working Paper 7586, World Bank Group, Development Economics Vice Presidency Operations and Strategy Team, 2016. <http://documents.worldbank.org/curated/en/909261467990967406/pdf/WPS7586.pdf> (Consulted in 11 January 2019)

[30] Saurabh Verma, Rajender Kumar and P.J. Philip, The Business of Counterfeit Drugs in India: A Critical Evaluation, *International Journal of Management and International Business Studies* , 2014, Volume 4, Number 2, pp. 141-148

[31] Moyo Nzololo And Roger Armand Makany, Economic Analysis Of Non-Deceptive Counterfeiting In Congo *Int.J.Eco.Res*.,2015, v6 i6, pp. 08 – 21.

[32]For more information, <https://medium.com/brandsecurity/why-instagram-has-become-the-biggest-platform-for-distribution-of-counterfeit-items-on-runet-and-8e20f533a7bf> (Consulted in 11 January 2019)

[33] Carolyn Deere Birkbeck, The Politics of Intellectual Property Reform in Developing Countries: The Relevance of the World Intellectual Property Organization, *Oxford University Press,* 2009, pp. 111-133.

## 2.2. Brief Explanation of the UDRP

### 2.2.1 The Industry of Domain Names

To understand how the UDRP works, it is needed to see how trademarks and usage of websites may conflict on the internet. First of all, every internet user has to connect to the internet over devices. Regardless of the types, every device connects to a website which has a specific internet protocol address known as IP address. IP addresses consist of numbers such as 873.4.245.875. Due to the fact that remembering these IP addresses is very hard for people, taking the number of websites into the consideration, the necessity of domain names has become clear. While the alphanumeric format was being used, the legal dispute related to trademarks rose gradually in parallel with the spread of the usage of websites in almost every sector[34].

Domains serve as brands, they are directly related to the people`s or companies` reputation. Based on this idea, differences in domain prices could happen because of the brand potential inherent in the domain name. The creations of domain names are similar with trademarks` one, since, being catchy and easy-to-remember names may provide marketing advantages. Therefore, there is a gradual rise in the number of domain registrations. According to the Verisign domain industry brief[35], the third quarter of 2018 closed with approximately 342.4 million domain name registrations across all top-level domains (TLDs), an increase of approximately 2.6 million domain name registrations, or 0.8 per cent, compared to the second quarter of 2018. Domain name registrations have grown by approximately 11.7 million, or 3.5 per cent, year over year. The domain name industry has been found attractive by a number of entrepreneurs in bad faith who plan to abuse the intellectual property rights in order to make profit via domain name monetization.[36]

Given the massive size of the domain market and the participation of ``bad players``, it is seen that thousands of conflicts most probably emerged among trademarks, corporate names, personal names and meta elements that have been in websites. In order to solve domain names disputes, the Uniform Domain Name Dispute Resolution Policy (UDRP) was established by ICANN. This policy[37] is basically the legal framework run by the WIPO Arbitration and Mediation Center for the resolution of disputes between a domain name registrant and a third party.

### 2.2.2 The Process of the UDRP

According to paragraph 15 (b) of the UDRP policy, the Panel shall forward its decision on the complaint to the Provider within fourteen days of its appointment. The decision of the panel is the final decision before the WIPO. There is no appeal chance against the

[34] Trademark issues related to Internet Domain Names, <https://blog.ipleaders.in/trademark-issues-related-to-internet-domain-names/> (Consulted in 26 April 2019)
[35] The Domain Name Industry Brief, The Verisign Domain Report, 2018, <https://www.verisign.com/assets/domain-name-report-Q32018.pdf> (Consulted in 11 January 2019)
[36] Torsten Bettinger, Allegra Waddell, *Domain Name Law and Practice An International Handbook*, Oxford University Press, Oxford, 2015 p. 140.
[37] For more information regarding the Uniform Domain Name Dispute Resolution Policy (UDRP) https://www.wipo.int/amc/en/domains/guide/#a

panel decision. However, parties are free to bring the panel decision to the national courts.

The panel or panels analyse three elements regarding the UDRP's three-prong test. The three elements[38] are present below;

(i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and
(ii) you have no rights or legitimate interests in respect of the domain name; and
(iii) your domain name has been registered and is being used in bad faith.
The second and the third elements are going to be analysed in chapter 3, particularly with the effect of the GDPR.

The UDRP is not applicable for all type of domain names, thus, in the next section some types of domain names and the differences in the requirements of domain registrations will be explained in order to clarify how the crash between trademarks and domain names comes to exist.

### 2.2.3. The Importance of Domain Names Types

Each domain name consists of at least two components: Top-level domains (TLDs) structure the overall name space into a limited number of subsets that either have global scope (gTLD- generic top level domain), such as COM, NET, ORG, or that are country specific (ccTLD- country code top level domain), such as DE, FR, NL[39].

There is an important issue between the relationship of the TLD administration and the political jurisdictions. A domain name is part of the administrative authority over the internet, in such it is much more than just a name or a label.[40] Country code top level domains are under control of local authorities. More specifically, requirements to have a ccTLD are changeable from country to country, which causes legal uncertainty in the matter of domain registration and applicable law in a dispute.

According to ICANN, every national ccTLD provider has the right to set their own rules for registration and therefore also for dispute resolution. For instance, in Japan Individuals can register a ``.jp`` domain name if they reside in Japan or have a company that is located there - the registrant contact country must be Japan.[41] In Israel, a latin domain name with ``.il`` must not be identical to any existing Top Level Domain name in the global Internet (at the time the application is submitted).[42] It is seen that domain registration with the country code is so far away from harmonisation.

---

[38] Uniform Domain Name Dispute Resolution Policy, paragraph 4(a)
[39] Thies Lindenthal, Valuable Words: The Price Dynamics of Internet Domain Names, *Journal Of The Association For Information Science And Technology, Massachusetts Institute of Technology*, 2014 65(5), pp . 869–881.
[40] Milton L Mueller, The battle over Internet domain names. Global or national TLDs? *Telecommunication Policy*, 1998, Vol. 22, No. 2, pp. 89—107.
[41] .jp domain registration, https://uk.godaddy.com/help/about-jp-domains-20219
[42] Rules for the Allocation of Domain Names Under the Israel Country Code Top Level Domain (".IL") <https://www.isoc.org.il/files/docs/ISOC-IL_Registration_Rules_v1.6_ENGLISH_-_18.12.2017.pdf > (Consulted in 2 March 2019)

With regard to the laws applicable to ccTLD, the proceedings are applied in accordance with the national law of the country of origin (for example, com.us is according to American laws). ICANN maintains the role of coordinating and ensuring the stability and security of the domain name system in relation to gTLDs, while the registry and the relevant state authorities have the right to self-determination in important administration process in respect of ccTLDs.[43]

Another importance of the types of domains is that in many jurisdictions, taking legal action against the domains that are gTLD is not always possible before national courts. Since, the local courts have to analyse and decide in the matter of governing law and venue. German courts acknowledge that they are authorized in case of damage to a protected trademark in Germany due to the website. If the website does not target the people in Germany or if the website is not activated, German courts may not be the authorised court. In comparative law, the international jurisdiction of the courts is determined according to whether the website of the used domain is unfair and whether the goods or services offered outside the internet are targeted to the customers in the country of the court.[44] This practise is also adopted by WIPO according to the Joint Recommendation Concerning Provisions on the Protection of Marks, and Other Industrial Property Rights in Signs, on the Internet.[45]

Even though a local court acknowledges the governing law and venue, the decision of the court may have limited effect due to the principle of territoriality. The decision related to gTLD is only enforceable within the origin country of the court. The IPR holder may try to make the decision valid in other countries over the process of recognition and enforcement. However, the processes are mostly required to new trials which are long and costly. One of the classic examples of these difficulties is the case of Prince PLC (hereinafter referred to as Prince) v. Prince Sports Group Inc.(hereinafter referred to as Prince Sport), an US manufacturer had several trademarks registered with ``Prince`` in the USA and the UK. The American company learned that the ``prince.com" domain name was already registered by Prince plc from the UK. Prince Sports filed a suit in the US under US trademark law, while Prince filed a suit in London under the UK trademark law. [46] Both companies were seeking injunctions against the other, demanding the takeover of domain name ``prince.com." Consequently, the UK court issued an injunction against Prince Sport in order to stop demands against Prince. However, the court refused to give an injunction to stop the lawsuit in the US court, since if it gave, it would mean the violation of the jurisdiction of the US court. At the end, the case was subsequently settled and resulted with

[43] See Domain Name Law and Practice An International Handbook, p. 1509
[44] Renck, Adreas W; Kennzeichenrechte versus Domain Names-Eine Analyse der Rechtsprechung, *Neue Juristische Wochenschrift (NJW)*, 1999, 49, pp. 3587-3590.
[45] Joint Recommendation Concerning Provisions on the Protection of Marks, and Other Industrial Property Rights in Signs, on the Internet, adopted by the Assembly of the Paris Union for the Protection of Industrial Property and the General Assembly of the World Intellectual Property Organization (WIPO), 2001
<https://www.wipo.int/edocs/pubdocs/en/wipo_pub_845.pdf> (Consulted in 11 February 2019)
[46] Michael T. Zugelder, Theresa B. Flaherty and James P. Johnson, Legal issues associated with international Internet marketing, *International Marketing Review*, 2000, Vol. 17 Issue: 3, pp.253-271.

dismissing Prince Sports`s lawsuit in US and Prince retains the ownership of the domain name.[47]

The expectation arises that, with the introduction of a new gTLD program, domain name prices will become lower and that it will become easier for consumers and companies to register a domain name of their liking.[48] For instance, new gTLD can be .GLOBAL, .ORGANIC, .REALTOR, .TOP, .XYZ, .THEATRE, .LONDON, WIEN and so on.[49] It means that the possibility of being conflicts on domain names is getting higher due to the abovementioned new program.

Consequently, taking into account the jurisdiction, applicable law, cost in national litigation, enforcement problems and differences in the requirements of domain registrations, it is seen that the UDRP provides an effective and easy protection for the IPRs holders.

[47] Id., p. 262.
[48] *Bettinger* (n 36).
[49] For more examples https://newgtlds.icann.org/en/announcements-and-media/case-studies

# Chapter 3. What are things that are going to change after the GDRP in the UDRP process? And how can the UDRP survive?

## 3.1 What are the impacts of the GDRP?

### 3.1.1. Before the GDPR

To understand what the things that changed after the GDRP in the UDRP process are, we firstly have to look at the system before the GDPR.

To begin with an example, Company A is a rights holder and one of its trademarks is being used without its permission as a domain name which is registered by Company B, which is a registrar company. The registrant that applies to company B in order to obtain a domain name is company C. In this case, the third party is company A and its legitimate interest is protecting its IPRs. The registrars collect the personal data in order to register the domain name on behalf of their client names. The registrars have agreements with ICANN and this agreement requires them to publish data such as the names and email addresses through their service.[50] The data was published in the WHOIS database and any party like Company A has access right to learn the registrant`s name and contact details.

Actually, early on, WHOIS was thought of as a communication way between the user and a technician when there was a technical problem such as internet connectivity or functionality problems. However, later, this database has been started to be used as a way of investigation by law enforcement officials, owners of IPRs.[51] Later on, WHOIS became a practical tool among law practitioners. WHOIS is so important because it is used for; researching whether a domain name is available, contacting a domain name registrant on matters related to the protection and enforcement of intellectual property rights and any other law enforcement such as fraud.[52]

When an IPRs holder detects an infringement in a domain name, the holder could learn the owner's details and he can contact the opposite party. Obtaining the information of the domain name owner provides opportunities to send cease and desist letters, to negotiate about the use of the domain name and to offer the purchase of the domain name. In other words, apart from the litigation or the UDRP process, it supplies many choices in order to resolve the dispute. However, after the GDRP, accessing the information of domain name owners is no longer possible. In this chapter, the impacts of the impossibility to access the data on the UDRP process will be analysed.

[50] 2013 Registrar Accreditation Agreement, 3.3 Public Access to Data on Registered Names https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

[51] Internet Management, Prevalence of False Contact Information for Registered Domain Names, United States Government Accountability Office, 2005 < https://www.gao.gov/new.items/d06165.pdf> (Consulted in 11 February 2019)

[52] What is WHOIS data used for? < https://whois.icann.org/en/what-whois-data-used> (Consulted in 4 March 2019)

### 3.1.2 After the GDRP

The GDPR is a new regulation of data protection that basically provides more safeguards on personal data and tighter controls on using personal data in European Union. Moreover, the GDRP includes stricter provisions for transfer of personal data outside of the EU.[53] This strict control causes problems in the litigation process, since an applicant or a complaint needs the opposite party`s information in order to initiate the process.

The problem in the UDRP is that registrar companies reject to share their clients` information due to the fact that a lack of lawful processing circumstances after the GDPR came into force. For instance GoDaddy, which is the biggest registrar company, has announced that they are not going to share the information of their clients with the WHOIS database.[54] A Dutch registrar company, FRLRegistry B.V, has sent a letter to the president of ICAAN and it indicated that the registration agreement which requires the obligation to publish registrants` data is an obvious breach of the GDPR. The obligation for disclosure of their clients` data cannot be considered as breach of the registration agreement between them and the ICAAN. The clause is an invalid contractual clause due to the fact that under the Dutch law a clause that violates the law is null.[55]

Article 6 of the GDRP sets out the circumstances of lawful processing of personal data. From these circumstances, paragraph (a), (b)and (f) can be a ground for personal data disclosure in order to solve the WHOIS database dilemma. These grounds are:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

In the event of these three circumstances, it needs to be applied to legal assessments for each processing of personal data. The conditions of lawful processing should be evaluated with data protection principles such as data minimisation and purpose limitation.[56] In other words, the mere existence of these circumstances does not legitimize the data processing. In practice, all of them have some specific difficulties which will be analysed in the next section.

[53] the GDPR Article 45, 46, 47, 48, 49, 50.
[54] https://au.godaddy.com/help/gdpr-faq-27923
[55] The letter from the attorney of FRL Registry B.V to ICANN,09.10.2017 <https://www.icann.org/en/system/files/correspondence/sprey-to-Marby-9oct17-en.pdf> (Consulted in 18 February 2019)
[56] Hamilton GDPR Memorandum part 1, Thomas Nygren and Pontus Stenbeck, Hamilton Advokatbyrå, 16 October 2017. < https://www.icann.org/en/system/files/files/gdpr-memorandum-part1-16oct17-en.pdf> (Consulted in 29 May 2019)

In order to analyse paragraph (a), (b) and (f) which give the possibility for the lawful processing of data, it need to be explained who are the controller and third party. It may be said that the controller is ICANN, since, according to Article 4 of the GDPR, the controller is ``*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.*`` The third party may be IPRs holders that ask for the information of the owner's domain name in order to initiate an action.

#### 3.1.2.1. Article 6 Paragraph (a); The Consent of The Registrant For The Data Disclosure

In order to obtain the consent from the domain names owner, ICANN may consider revising the registration agreement which is compulsory to be accepted when a request is done to register a domain name. The consent can be laid down as a condition in a registration of a domain name. However, this sort of consent might not be valid consent in terms of data protection law, since Article 7 of the GDRP specified that the consent should be freely given[57].

According to recital 43 of the GDRP, ``In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation``. Therefore, even though the ICANN may obtain the consent by revising the registration agreement, the consent might not be considered as a consent which is given for a specific case. An alteration in the registration agreement for content may only provide a bundle consent, since the word ``specific`` in recital 43 of the GDPR refers to the purpose of data processing. Therefore, the consent must relate to each of the transactions. If there is more than one purpose of data processing, then the consent should be given for each of them.[58] In the matter of the WHOIS, when registrants registrar a domain name, they have never been informed that their personal data is taken in order to be used in the UDRP system. According to ICANN, WHOIS data can be used for many legitimate purposes but none of them is explicitly related to the UDRP.[59]

Regarding paragraph (a)[60], the requirement of the consent, expecting from the parties to disclose their identities to be a defendant or to be party of a UDRP complaint will not be a realistic.

Finally, ICANN has mentioned the legitimate interest for the UDRP process in the Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy

[57] GDPR Conditions for consent, Art. 7/4 When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.
[58] Bojana Kostic and Emmanuel Vargas Penagos, The freely given consent and the "bundling" provision under the GDPR, *AFL*, 2017, 4.. PP. 217-222.
[59] What is WHOIS data used for? < https://whois.icann.org/en/what-whois-data-used> (Consulted in 4 March 2019)
[60] The General Data Protection Regulation, Article 6 lit. (b) of the GDPR

Development Process[61] (hereinafter Final report of the temporary specification). It has emphasised that there are two lawful bases in collecting data that are going to be analysed below.

**ICANN PURPOSE:**
Coordinate, operationalize and facilitate policies for resolution of disputes regarding or relating to the registration of domain names (as opposed to the use of such domain names), namely, the UDRP, URS, PDDRP, RRDRP and future-developed domain name registration-related dispute procedures for which it is established that the processing of personal data is necessary

| Processing Activity | Responsible Party: | Lawful Basis: |
|---|---|---|
| Collection | ICANN<br>Registrars | 6(1)(b) for Registrars<br>6(1)(f) for Registries |
| Transmission from Rr to Ry | ICANN<br>Registries<br>Registrars | 6(1)(b) for Registrars<br>6(1)(f) for Registries |
| Transmission to dispute resolution providers | ICANN<br>Registries<br>Registrars Dispute Resolution Provider – Processor or independent controller | 6(1)(b) for Registrars<br>6(1)(f) for Registries and ICANN |

**Table 1 Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process**

### 3.1.2.2. Article 6 paragraph (b); The necessity for the performance of a contract

According to ICANN`s Bylaws[62], ICANN`s policies and agreements have also included the responsibilities of ICANN regarding WHOIS database. According to paragraph (b)[63] the parties can agree on the data sharing with the third parties under certain circumstances in the event of an agreement. However, contractual obligations regarding the data collection cannot be considered as lawful grounds by the data protection authorities and courts. The letter from Article 29 Data Protection Working Party on 6th of December 2017[64] states that ICANN cannot appeal to any grounds of lawful data processing, since:

- `the consent` regarding the domain name cannot be considered as `freely given consent` (see the previous section) ,
- individuals who are the domain owner are not party of the contract between ICANN and registrar companies,
- there is no legitimate interest in making all the data available in an online platform.

[61] Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process, ICANN, 20 February 2019 <https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf> (Consulted in 19 April 2019)
[62] ICANN, Bylaws For Internet Corporation For Assigned Names And Numbers, As amended 18 June 2018.)
[63] The General Data Protection Regulation, Article 6 lit. (b) of the GDPR
[64] Article 29 Data Protection Working Party letter to ICANN, 06 December 2017 <https://www.icann.org/en/system/files/correspondence/falque-pierrotin-to-chalaby-marby-06Dec17-en.pdf>(Consulted in 8 May 2019)

When the performance of a contract is referred to in this section, it means the contract between the registrant and registrar companies, not a contract between registrants and ICANN. Similar approaches have also been adopted by the German courts, which is going to be analysed in Chapter 4. I think, in order to rely on paragraph (b), ICANN needs to establish a contractual relationship with registrants. It requires an independent agreement from RAAs, since a RAA is a contract between registrars/registrar companies and ICANN. As it is seen, data subjects are not party of any contract with ICANN. On the other hand, the data minimisation principle is a key point in determining which data should be required. For instance, a provision which requires disclosure of the technical contact on the WHOIS might be violation of the data minimisation principle. Thus, it might be null despite the fact that contractual requirements exist, since technical data exists in order to get in contact with the domain name owner in the event of a technical problem (see section 4.1.1.). Therefore, the disclosure of this data would not contain a legitimate interest of a third party.

Without an agreement, the only possible way seems to introduce a new mechanism that provides limited access to the personal data in the event of legitimate interest which does override the data protection rights of individuals. On the other hand, if an independent agreement is executed between registrants and ICANN, the provision will explain under which circumstances the data of the domain owner will be shared with third parties. This provision should not conflict with the GDPR. Otherwise, there will be a risk of invalidity of the agreement. Today, even if there was an provision that requires the data sharing with ICANN, controllers would need to evaluate data disclosure requests respectively in terms of compliance with data protection principles.

#### 3.1.2.3 Article 6 Paragraph (f); The Legitimate Interest of IPRs Holders

There is no indication as to how to interpret the meaning of legitimate interest regarding the data processing by the data protection authorities after the GDPR. The regulation itself does not define `legitimate interest`. The characteristic of paragraph (f) contains a `catchall element`, thus, interest needs to be interpreted broadly[65]. Economic, non-material, factual interests should be accepted as legitimate interests[66]. This interpretation brings us to the point of the necessity of the balancing test, since the legitimate interest in data disclosure and privacy right of the data subject clashes. However, it is not clear which one is overriding. I am of the opinion that case law might be helpful in underpinning the legitimate interest of the data processing. Therefore, in this part, it needs to be analysed whether paragraph (f) [67] can find a place in case law related to limitations on the right to obtain personal data.

Processing registrants` data without their consent is clearly an interference with the registrants` rights, which are under the protection of Article 8 of the ECHR and Article 7 and 8 of the Charter. However, these rights are not absolute rights. In other words,

[65] GDPR Domain Industry Playbook, Association of the Internet Industry, Julia Garbaciok, Andreas Konrad, Martin Lose, Thomas Rickert, Jan Schlepper, Oliver Süme, 2017 < https://www.eco.de/wp-content/uploads/2017/12/20171208-DRAFT_eco_GDPR_Playbook.pdf> (Consulted in 29 May 2019)

[66] Ibid.

[67] The General Data Protection Regulation, Article 6 lit. (f) of the GDPR

people`s rights on their data may be restricted under certain circumstances. According to the CJEU judgement[68], processing personal data constitutes a lawful interference with the right to respect for private life, if the interference is in accordance with the law and is necessary in a democratic society for the interests of national security, public safety, the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.

The case law of the ECtHR and the CJEU have indicated similar requirements for a lawful interference.[69] Article 8 of the Charter allows us to apply step by step analysis of the interference. For this analysis, the questions that are needed to ask are these[70];

Has there been an interference with the Article 8 right? If the answer is yes, it will lead to these questions below:

1- Is the interference in accordance with the law?
2- Does it pursue a legitimate aim?
3- Is it necessary in a democratic society?

There is no doubt that personal data is under the protection of Article 8 of the ECHR.[71] Therefore, processing a registrant`s data of a domain name owner is an interference of Article 8. From this viewpoint, these 3 steps are needed to be in processing registrants` data for the WHOIS database. Regarding the UDRP, the balancing test will be required between right an effective remedy (Article 47 of Charter and Article 13 of ECHR), right to protection of property (Protocol 1, Article 1) and privacy of people (Article 7 and 8 of the Charter, Article 8 of ECHR).

To begin with ``being in accordance with the law``, which basically means that every country should have a domestic legislation which regulates the obligation for data sharing with the WHOIS. However, as it is mentioned in chapter 2, there is no harmonisation in the field of domain name registrations and further steps related to the registration. Moreover, the regulation for sharing data only exists for domain names with `.eu`.[72] For others, there are no specific regulations which explains which data is going to be accessible on WHOIS and which data is going to be limited accessible through the data disclosure request form. For instance, it is seen that registrar companies

[68] CJEU, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen [GC], 9 November 2010, para. 48.
[69] Handbook on European data protection law 2018 Edition, European Union Agency for Fundamental Rights and Council of Europe, European Court of Human Rights, Council of Europe, European Data Protection Supervisor, 2018.
<https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf> (Consulted in 8 May 2019)
[70] Protecting the right to respect for private and family life under the European Convention on Human Rights Council of Europe human rights handbooks, Council of Europe Strasbourg, 2012.
<https://www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf>(Consulted in 8 May 2019)
[71] ECtHR, S. And Marper v. The United Kingdom, Applications no. 30562/04 and 30566/04, 4 December 2008.
[72] Regulation (EU) 2019/517 of the European Parliament and of the Council of 19 March 2019 on the implementation and functioning of the .eu top-level domain name and amending and repealing Regulation (EC) No 733/2002 and repealing Commission Regulation (EC) No 874/2004

have been managing this matter with domain name registration agreements.[73] Germany has similar terms in the domain name registration process for `.de` top level domains. According to Section 7 paragraph 3 of Denic Domain Guidelines and Data Protection Information, DENIC will forward the domain owner's data to third parties who provide the legitimate interest on the personal data of the domain name owner.[74]

The question arising regarding this practice is: does having an ``agreement`` or ``guideline`` mean that the interference is in compliance with the law? The Court has made a broad comment in this matter. The justification of an intervention may be in different sources, not in a national legal regime, but also in professional codes of conduct, non-formal principles of law, European Union regulations or international treaties. On the other hand, other legal sources, which do not have accessibility, which are not characterized by administrative arrangements, which have a high degree of flexibility or discretionary power, do not usually have sufficient legal basis for the purposes of Article 8.[75] Therefore, it is not clear whether data processing based on a guideline or an agreement is considered as being in accordance with the law.

Regarding the legitimate interest that the interference should have, I think, the legitimate interest in data processing in the matter of the WHOIS database is protection of the intellectual property right. Accessing the personal data of the domain name owner is essential in the UDRP. Otherwise, IPRs holder might not obtain enough data in order to use effective ways to protect their rights, in which the states have positive obligations in ensuring. Therefore, the data processing pursue a legitimate aim.

The necessity of the interference in a democratic society should be interpreted with proportionality. Proportionality requires that the interference with the rights protected in the ECHR does not progress further than is necessary to fulfil the legitimate aim pursued.[76] In terms of the UDRP it can be claimed that the IP address or the address of the domain owner is not necessary to carry out the UDRP complaint in terms of proportionality.

Another important point which should be mentioned in balancing rights is the essence of right. Since, when the essence of a fundamental right is affected, it is concluded that

[73] ``As required by ICANN, this information must also be made publicly available by means of Whois, and that the registry operator may also be required to make this information publicly available by Whois.`` Section 5, Godaddy Domain Name Registration Agreement, last revised December 2019. <https://au.godaddy.com/legal/agreements/domain-name-registration-agreement> (Consulted in 29 May 2019)

[74] DENIC-Domainrichtlinien und Datenschutzhinweise https://www.denic.de/domains/de-domains/domainrichtlinien/

[75] Protecting the right to respect for private and family life under the European Convention on Human Rights Council of Europe human rights handbooks, p 37.

[76] Opinion on the application of the necessity and proportionality concepts and data protection within the law enforcement sector, WP 211, Article 29 Data Protection Working Party, 2014. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf>

there is a violation without doing the abovementioned balancing test.[77] According to Maja Brkan:

> ``*the essence sometimes referred to as the minimum, essential or absolute core of a right – represents the untouchable core or inner circle of a fundamental right that cannot be diminished, restricted or breached upon save for the right to lose its value either for the right holder or for society as a whole*.``[78]

In case law, when the personal data disclosure is demanded in order to protect IPRs the importance of balancing interest has been emphasised. For instance, Promusicae v. Telefónica de España case, Promusicae, a non-profit organization composed of producers and publishers of musical recordings in Spain, asked the European Court of Justice to order Telefonica to disclose personal data of its users, since the users were violating copyrighted works. The Court held that the Directives do not require member states to set up such obligations for data disclosure in order to initiate legal proceedings for the protection of intellectual property rights. However, member states should ensure a fair balance between the various fundamental rights.[79] Consequently, in order to reach the personal data, it is necessary to pass the balancing test successfully. To do that, it is important to prepare the arguments which prove the infringements of IPRs clearly. On the other hand, in order to prove an infringement and bad faith of the domain owner, you need the data. The whole situation gets into a vicious circle. This is the disadvantage of paragraph (f).

The UDRP is still possible regardless the data disclosure of the domain name after the GDPR comes into force. In these circumstances, it is going to be discussed what the panel of the UDRP may do to keep the effectiveness of the UDRP in the following chapter.

## 3.2. What Changes After The GDRP

### 3.2.1. The Changes In the Pre-UDRP Period

IPRs holders need to change their approaches in the Pre-UDRP steps. When the data is not available on the WHOIS database, IPRs holders have to do their own research in order to figure out who is running the website. For law enforcement parties in this research, I am of the opinion that the following tips may be helpful;

1- Despite the GDPR, the WHOIS database remains the most important tool for the UDPR, since the country where the domain name is registered may be a country where the GDPR is not applicable.

---

[77] Martin Scheinin, The Essence of Privacy and Varying Degrees of Intrusion, 2015 <https://verfassungsblog.de/the-essence-of-privacy-and-varying-degrees-of-intrusion-2/> (Consulted in 8 May 2019)

[78] Maastricht Faculty of Law Working Paper 2017-01, In search of the concept of essence of EU fundamental rights through the prism of data privacy, Maja Brkan, 2017. <https://cris.maastrichtuniversity.nl/portal/en/publications/in-search-of-the-concept-of-essence-of-eu-fundamental-rights-through-the-prism-of-data-privacy(dbe1c250-a01a-4b26-9ad7-02baeaae7e7a)/export.html> (Consulted in 8 March 2019)

[79] CJEU, Productores de Música de España (Promusicae) v. Telefónica de España SAU [GC], C-275/06, 29 January 2008.

2- It was clear that companies' information cannot be considered as personal data under the GDPR. However, employees and attorneys on behalf of companies may apply to registrars companies in order to reach to the protection under the GDPR. However, some information can be found in privacy policies and disclaimers terms of use of a website. Since, according to the e-commerce directive[80], the companies have to disclose the name of the service providers, the contact details of the service providers. In this way, third parties who have legitimate interest may reach some personal data in order to prepare an UDRP.

3- In the event of demanding the data disclosure from the registrars or filing a complaint to a competence data protection authority in order to use the personal data in UDRP, a declaratory lawsuit before Intellectual Property courts might be used as supportive documents in a request or a complaint. Since, neither data protection officers nor the employee of a registrar is the expert of the IP. Therefore, supportive arguments which shows the clear legitimate interest of the IP rights holder may need to be presented.

### 3.2.2. The Case Law in UDRP

43,197 UDRP proceedings have been performed since 1999, which is the date of the UDRP adaptation.[81] During the 20 years after 1999 the arbitrators of the UDRP have developed a specific case law[82], which serves the challenges that come with the technology and the internet. However, after the GDPR, the case law has to change and in this section, this change is going to be analysed.

WIPO has announced that it has been continuing to accept the UDRP without the information of the respondent.[83] However, it is undeniable the fact that it will be seen in the changing approaches of panels.

As it is mentioned in chapter 2, the complainant has to prove three elements that are mentioned in paragraph 4 (a) of the UDRP policy. The second element of the policy requires the complainant to prove that the respondent lacks legitimate interest in a dispute. According to my opinion, this burden was already heavy but after the GDPR, it is proven to become almost impossible, since complainants do not know any details about the respondent. In case law of the UDRP before the GDPR, the heaviness of this burden has been shifted to the respondent under some circumstances. In administrative panel decision with case number D2009-1015[84], the panel notes that ``the complainant bears the "general burden of proof" under paragraph 4(a)(ii) of the Policy, which burden shifts to the Respondent once the Complainant makes a *prima facie* showing that the Respondent lacks rights or legitimate interests.`` The meaning of ``prima facie`` is that the complainant has undertaken enough research and according to his knowledge, there

[80] Article 5 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000
[81] https://www.wipo.int/amc/en/domains/statistics/cases.jsp
[82] Here case law does mean the interpretations, since UDRP does not operate on a strict doctrine of precedent.
[83] Impact of Changes to Availability of WhoIs Data on the UDRP: WIPO Center Informal Q&A < https://wipo.int/amc/en/domains/gdpr/ >, (Consulted in 1 May 2019)
[84] WIPO Arbitration and Mediation Center, Panelist Haig Oghigian, AXA SA v. Value Domain Case No. D2009-1015, Administrative Panel Decision, 22 September 2009.

is no legitimate interest of the complaint. Then the burden shifts to the respondent.[85] This UDRP practise is needed to be interpreted more flexibly. When the disputed domain is not available in the WHOIS due to the GDPR, the complainant should be excluded automatically from his burden under paragraph 4(a)(ii) of the Policy.

According to the consensus view of the WIPO, it is accepted that although the use of a privacy or surrogate recording service is not a sign of bad faith on its own, the manner in which this service is used may in some cases be a factor of malicious intent.[86] However, concealing the details cannot be accepted as a sign of ``bad faith`` after the GDPR. A similar approach was also adopted for the registrant that uses a privacy or proxy service. This service is known for blocking the data or delaying the data disclosure on the WHOIS system. According to WIPO`s announcement[87] and the decision[88], using a privacy or proxy service has been interpreted as an indication of bad faith. As it is mentioned in chapter 3.1.2, people have the right not to give consent on their personal data processing in the WHOIS database. Therefore, exercising a right cannot be evaluated as a factor in determining whether a domain registrant is in bad faith or not.

Telstra doctrine has been adopted widely in the UDRP decisions.[89] The principle is justified, when it is used only in isolation in the domain name of a trademark or in cases where the trademark of the complaint is well known and it is truly unthinkable that the respondent registers the domain name in good faith.[90] In this doctrine, silence or not responding of the respondent is interpreted as the respondent's acknowledgement for the recognition of the trademark. However, this doctrine should no longer be possible to apply to some cases after the GDRP. For instance; in the decision of WIPO[91], it has been applied to Telstra doctrine failing in responding to the complainant's letters and e-mails have been claimed as a factor of being in bad faith. In a decision of WIPO[92], continued concealment of the personal data has been accepted as an element of bad faith. In another decision of WIPO[93], it has been considered that not providing evidence of any actual good faith about the usage of domain name is a sign of bad faith. In the decision with number D2009-0266[94], the panel held that the respondent did not reply to

[85] Bettinger, Waddell p. 1329.
[86] https://www.wipo.int/amc/en/domains/search/overview2.0/#39
[87] WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Third Edition ("WIPO Overview 3.0"), WIPO, 2017 <https://wipo.int/amc/en/domains/search/overview3.0/#item36> (Consulted in 16 April 2019)
[88] WIPO Arbitration and Mediation Center, Panelist Reyes Campello Estebaranz, Compagnie Générale des Etablissements Michelin v. Balticsea LLC, Case No. D 2017-0308, Administrative Panel Decision, 10 April 2017.
[89] WIPO Arbitration and Mediation Center, Panelist M. Scott Donahey, Alleghany Pharmacal Corporation v. Hair for Life case No D 2003-1045, Administrative Panel Decision, 26 February 2014.
[90] *Bettinger, Waddell* (n 36)
[91] WIPO Arbitration and Mediation Center, Panelist Torsten Bettinger, Stanworth Development Limited v. Dr. Ricardo Vasquez Case No D 2008-0943, Administrative Panel Decision, 20 August 2008.
[92] WIPO Arbitration and Mediation Center, Panelist Luca Barbero, M/s Genpact Limited v. Contact Privacy Inc. / self, Case no D 2012-0307, Administrative Panel Decision, 10 April 2012.
[93] WIPO Arbitration and Mediation Center, Panelist Alvaro Loureiro Oliveira, Intesa Sanpaolo S.p.A. v. Croitoru Daniel Case D 2012- 1113, Administrative Panel Decision, 20 August 2012.
[94] WIPO Arbitration and Mediation Center, Panelist Jeffrey M. Samuels, Pearson Education, Inc v. CTP Internacional; Private Registration at Directi Internet Solutions Pvt. Ltd. and <scottforesmanandcompany.com>

the cease and desist letter which is sent by the complainant. Failing in replying is also accepted as a factor in detecting the bad faith of the respondent.

There is no clear plan or guideline about the arbiters` possible approaches. However, the WIPO has given the first signal related to their approaches which might change. According to their explanation in the `question and answer part` on their website[95], it is stated that;

> `*It is anticipated that the overarching consolidation standard itself will remain unchanged (as will the various consideration factors), although it is possible that in the absence of registrant contact information in the public WHOIS, Panels may increasingly focus on other indicia of common control.*`

To understand the meaning of `common control`, the case law needs to be analysed. The common control has been used when the respondent controls multiple domain names. The panel may conclude that there is one owner or single network, entity that controls all domain names[96]. As it is understood, `common control` is only a matter when there is more than one respondent. In other words, it does not provide a helpful consideration that covers all the matters in the UDRP which are being affected by the GDPR. Moreover, according to the WIPO overview 3.0 section 4[97], which factors should be taken into the account are explained when the panels evaluate whether there is a `common control`. However, the analysis of some recommended factors is also not possible, since the data which is recommended for `common control` analysis is not available after the GDPR.

Instead of preparing clear guidelines for panels, the ICANN was struggling to revoke the GDPR effects on the WHOIS by taking legal actions against the registrar companies. In addition to this, they have announced a new project called `temporary specification`. With this project, they aim to provide solutions to keep the UDRP in accordance with the GDPR. In the next chapter, the steps of the ICANN will be analysed.

---

Case No D 2009-0266, Administrative Panel Decision, 11 May 2009.

[95] https://wipo.int/amc/en/domains/gdpr/

[96] WIPO Arbitration and Mediation Center, Panelist Karen Fong, F. Hoffmann-La Roche AG v. Konayem Temirtassova, Tigran Movsisyan and the others case no D 2015-0984, Administrative Panel Decision, 7 September 2015.

[97] *WIPO Overview 3.0.* (n 87)

# Chapter 4. ICANN`s Steps To Save The UDRP

## 4.1. The Court Actions

### 4.1.1. ICANN`s Injunction Demand against the Registrar Company

After the GDPR came into force in Europe, EPAG, which is a German registrar company, informed the ICANN that the company will no longer provide administrative and technical contact information because it believes that the collection of this data would be a violation of the rules of the GDPR. After it, ICANN announced that they are filing a lawsuit in Germany to further clarify that ICANN can continue to collect data for the WHOIS system. [98]

Before the Regional Court of Bonn in Germany, on 25th of May 2018 when the GDPR came into the force, ICANN asked for an injunction that prohibits EPAG from renouncing data collection for technical contacts (hereinafter Tech- C) and administrative contacts (hereinafter Admin-C) that they were collecting during internet domain registrations.[99] ICANN hoped to avoid contractual difficulties with registrars around the world to save time while developing a new version or model in accordance with the GDPR legislation by filing an injunction.

What are the claims of ICANN in this case? According to the petition of ICANN[100] for an injunction before the region court of Bonn, the main arguments of ICANN are;

1- ICANN puts forward the public interest in doing its duties by using the WHOIS database. Firstly, ICANN emphasised that it is a non-profit public benefit corporation. Secondly, ICANN`s duty, which is especially ensuring the stability and secureness of the internet has been stated. ICANN claimed that it also establishes the minimum requirements for WHOIS data. Therefore it makes the availability of WHOIS information certain in order to protect internet stability and safety and to contribute other legitimate public interest uses.

2- The defendant is under the contractual obligation due to the agreement with ICANN. One of the contractor's contractual obligations is to collect and store the specific registration data requested from its clients. Access to this data is required for a stable and safe way to run the domain name system, as well as a method to detect customers who may cause technical problems and legal issues with domain names and/or contents. Hence, the provisions of the GDPR do not hinder the defendant from collecting the data from its customers.

3- WHOIS is a decentralized database that allows end users to obtain contact information from registered Internet resources, such as domain names and Internet protocol addresses, for the protection of industrial property rights. The service provided

[98] https://www.icann.org/news/announcement-2018-05-25-en
[99] A preliminary injunction demand of ICANN against EPAG Domain services GmbH before Regional Court of Bonn, 25 May 2018.
<https://www.icann.org/en/system/files/files/litigation-icann-v-epag-request-prelim-injunction-redacted-25may18-en.pdf> (consulted in 9 April 2019)
[100] Ibid.

by the WHOIS system is especially important for those dealing with trademark issues, fraud and abuse.

WHOIS provides information about the availability of a particular domain for its registration. With WHOIS it can be checked which domain name is still available so that market participants may shape their trademark strategies accordingly. The chance to find out a domain name registrant who infringes a trademark is also with use of the WHOIS database. In both cases, obtaining contact information related to these domain names opens up an opportunity for intellectual property owners to communicate with those who registered the domain name to handle the violation.

4- WHOIS data plays a crucial role in an online criminal investigation. Information in the WHOIS system may be used as search terms elsewhere. For example, IP addresses in the domain name system and e-mail address databases ensured by anti-spam organizations can help lawmakers to get a larger picture of the activities of perpetrators.

5- On 17th of May 2018, the ICANN Board of Directors agreed on the "Temporary Specification``, a unified interim model providing a mutual system for registration data guide services that would not violate the GDPR. Temporary specification will be analysed further in the section 4.2.. With this model, ICANN will provide a legal basis in order to continue to keep the following data which is mentioned in the registrar accreditation agreement (hereinafter RAA) in subsections between 3.3.1.1 and 3.3.1.8[101]:

- The name of the registered name,
- The names of the primary and secondary nameserver(s) for the registered name.
- The identity of the registrar,
- The original creation date of the registration,
- The expiration date of the registration,
- The name and postal address of the registered name holder,
- The name, postal address, e-mail address, voice telephone number and fax number of the administrative contact for the registered name,
- The name, postal address, e-mail address, voice telephone number and fax number of the technical contact for the registered name.

6- The RAA necessitates the collection of data in order to provide communication when it is needed. There are two types of contact details, technical contact and administrative contact. Technical contact (hereinafter Tech-C) is the contact person in case of technical problems with the domain name. Administrative contact (hereinafter Admin-C) is the person or organization that has been granted the administrative control of the domain name such as access to the domain, changing the contact and transferring the domain name to another party.

[101] Section 3.3. of 2013 Registrar Accreditation Agreement, ICANN, 17 September 2013 https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa

7- The data of Tech-C and Admin-C might not be considered as personal data. Since, according to GDPR Article 1/1 ;

``*This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data*.``

At this point, the defendant, EPAG aims to justify the fact that the data is not collected without examining in detail whether the data refers to Tech-C or Admin-C personal data.

8- In the event that the Tech-C or Admin-C data is personal data, the collection of the data is permitted on the basis of the consent of the relevant data, in particular Article 6 (1) (a) of the GDPR. The defendant does not wish to obtain consent from the Tech-C or Admin- C to receive his data in order to comply with GDPR. It is hard to understand why the defendant does not seek this option.

9- The collection of data is necessary for the performance of a contract. The position of the Tech-C or the Admin-C is an important factor for the registrant. The registrant has to nominate tasks associated with registered domain names.

10- The trademark registration system has been shown as an example where the data of an applicant or the owner of a trademark has been published online. In the European trademark registration system, all data relating to a registered European trademark, including all contact details and legal representatives of a trademark owner including all correspondence and legal decisions regarding this trademark are available online without any restriction. The reason of this data disclosure online is not hard to understand. Law regimes enforce legal provisions that require the collection and publication of relevant data. These legal provisions mean the need for data collection. Therefore, the GDPR should not affect the lawfulness of the collection of such data.

11- The collection of the data does not conflict with the data minimisation principle. If the action is to be carried out to fulfil the legitimate aim, this step will be legal in accordance with the GDPR. The circumstances that can be applicable for the WHOIS database according to paragraph (a), (b) and (f) of Article 6 of GDPR.

12- Regarding the injunction relief, the applicant established the injunction demand based on the contractual relationship. More importantly, the defendant party may delete the data of the Admin- C and the Tech-C within short time. The reason behind this deletion of the data is that collecting the data is no longer necessary under the GDPR, but it is still a requirement due to the contract which is binder for the applicant and the defendant. Failure of the defendant to comply with the contractual obligations will induce irreparable damages. Once the defendant does not collect the Admin-C and the Tech-C data, this data is lost. Temporary specification system will provide a solution and will make it possible that the defendant is no longer obliged to open the data of the Admin-C and the Tech- C to the public.

In the reply petition of the defendant[102], it is briefly claimed that collecting the technical and administrative data violates the GDPR, particularly GDPR Article 5 (1) c which regulates the data minimisation principle and Article 25 which regulates the data protection by default and design. It is also stated that the defendant party is no longer under the obligation that the defendant had before the GDPR. Since the obligation is not in compliance with the applicable law.

### 4.1.2. The Rejection of the Injunction by The Regional Court of Bonn

The injunction was rejected by the regional court of Bonn on the 29th of May 2018.[103] The grounds of the courts are:

1- According to Section 3.7.2, the Registrar Accreditation Agreement of ICANN[104], the registrars must comply with applicable law and official regulations. At this point, the applicant may only expect or request the observance of the contract in accordance with the principle of loyalty.

2- The applicant has not proved that the retention of the owner`s personal data is indispensable for the purposes of the applicant, which continues to be collected and stored in an indispensable manner. The Tech-C and the Admin–C do not have to be different persons. They can also be the owner of the domain. Therefore the court could not see why the data of the person who is responsible for the website is not enough or why more is needed for the ICANN. More importantly, it should be taken into account that the same personal data can be used in all three categories.

3- In previous practice, one data set was collected instead of three different categories (the owner, Tech-C and Admin-C) and the demand of registration was not denied because of the lack of the data. In addition to this, if it was possible to register with only a domain name, then this should still be possible after the GDPR. The practise in the past is a clue that shows that the data that went beyond the domain name owner was not actually required.

4- The relation between the legal basis of the trademark registration system based on international agreements and the WHOIS database system is missing.

### 4.1.3. The Appeal of ICANN Against the Refusal On Injunction

ICANN appealed to lift the decision of the Regional Court of Bonn with the docket no 10 O 171/18. According to the immediate appeal petition of ICANN[105], the grounds of the appeal are:

---

[102] The Regional Court of Bonn the docket-no. 10 O 171/18, f Internet Corporation for Assigned Names and Numbers (ICANN) v. EPAG Domain services GmbH, Court Order In the preliminary injunction proceedings, 29 May 2018.
[103] Ibid.
[104] Section 3.7.2 of the Registrar Accreditation Agreement of ICANN. https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa
[105] The immediate Appeal Petition to Regional Court of Bonn 10th Civil Chamber, ICANN v. EPAG Domain services GmbH, 13 June 2018. <https://www.icann.org/en/system/files/files/litigation-icann-v-epag-immediate-appeal-redacted-13jun18-en.pdf> (Consulted in 15.05.2019)

1- The court of first instance only took into the consideration the universal legal principle which is that contractual obligations cannot go beyond the applicable law. However, these obligations that come from the RAA do not constitute a violation of the applicable law based on the argument in paragraph 8 and 12 in section 1.1. of chapter 4.

2- Processing the data of the Admin- C and the Tech- C is lawful. First of all, the information about the Admin-C and Tech-C does not need to be about real persons. It can be about legal entities or a representative. The GDPR only applies when the subjects are a natural person. Recital 14 of the GDPR clarifies by stating;

> `*This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.*`

However, regardless whether the data of the Admin-C and the Tech-C can be considered as personal data and/or regardless whether the data can be processed with the consent of the data subject, in any case the defendant rejected collecting the data.

3- The court has not evaluated the data processing in accordance with its legitimate purpose. This decision shows that the court does not understand properly what the meaning of `legitimate purpose` in collecting the data is. ICANN has many legitimate interests in collecting the data. The first one is delegating the task as it is mentioned in paragraph 9 in section 1.1. of chapter 4. The second legitimate interest of both the registrant and the third party is that the Admin-C and the Tech-C provide an opportunity for the registrant to effectively combat with abusive actions (examples such as criminal activities are explained in paragraph 4 in section 1.1.). Thirdly, in the UDRP procedure, the proof of the effective communication is also provided by delivering the complaint to the respondent according to the Admin-C and the Tech-C. In addition to this, the Admin-C is responsible to monitor according to the jurisdiction of the federal court of justice, thus, it can be liable due to a trademark violation. The Admin-C is also responsible for transferring domains. Therefore, respondents may need to get in contact with the Admin-C. For instance, In Germany in the event of a foreign domain owner, the Admin-C is a local contract person who can act as the authorized representative of the domain name owner. It can be communicated more easily than the domain owner who is domiciled in other countries. The fourth legitimate interest is related to trademark protection in dealing with the sale of counterfeiting goods online.

4- The court held that the collection of data including the Admin-C and the Tech-C violates the data minimization principle. This principle has three requirements. Firstly, the data should be related to the aim of collecting data. Secondly, the collected data should be limited to what is necessary in achieving the goal. This moves beyond the suitability of the data for the purpose and it requires consideration of whether the processing of the data in this extent is proportionate. In this case, only the data leading to the identification of the Admin-C and Tech-C was being collected in order to communicate in the case of legal necessity. Thirdly, according to Article 6 of the GDPR, legitimate interest of the controller or a third party is required for data

processing. The legitimate interests of the controller or a third party should be accepted widely. For instance, fraud prevention[106], marketing or network information security[107] might be considered as legitimate interests. It is mentioned in section 1.1. of chapter 4, particularly in paragraph 3, 4, 6 and 9.

5- When evaluating the legitimate interest, the court needs to analyse from the broad perspective. According to the guidelines on the application and setting of administrative fines for the purposes of regulation 2016/679, that is adopted on 3rd of October 2017[108], Art. 29 working party has referred to the previous report regarding the `purpose limitation`. On 2nd of April 2013, Art. 29 working party reported an in-depth view of the ``purpose limitation`` principle[109] (Hereinafter WP 203). In WP 203, this principle has stated;

`` *The requirement of legitimacy means that the purposes must be 'in accordance with the law' in the broadest sense. This includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts.*

*Within the confines of law, other elements such as customs, codes of conduct, codes of ethics,* **contractual arrangements**, *and the general context and facts of the case, may also be considered when determining whether a particular purpose is legitimate. This will include the nature of the underlying relationship between the controller and the data subjects, whether it be commercial or otherwise.*``

6- The specified purpose of the collection of personal data has been emphasised with the same arguments which are mentioned in paragraph 3 and 4 of section 1.1. of chapter 4.

7- Temporary specification by ICANN provides solutions by redacting the data. Temporary specification will be analysed in section 4.2.

8- RAA provides that the data processing is only lawful if it is based on the consents. Since Section 3.7.7.6. of the RAA states:

`*The Registered Name Holder shall represent that notice has been provided equivalent to that described in Subsection 3.7.7.4 to any third-party individuals whose Personal Data are supplied to Registrar by the Registered Name Holder, and that the*

[106] The General Data Protection Regulation, Recital 47
[107] The General Data Protection Regulation, Recital 49
[108] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Article 29 Data Protection Working Party 17/EN WP 253, 3 October 2017. <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237> (Consulting in 5 April 2019)
[109] Opinion 03/2013 on purpose limitation, Article 29 Data Protection Working Party, 00569/13/EN WP 203,
2 April 2013
<https://ec.europa.eu/justice/article29/documentation/opinionrecommendation/files/2013/wp203_en.pdf> (Consulting in 5 April 2019)

*Registered Name Holder has obtained consent equivalent to that referred to in Subsection 3.7.7.5 of any such third-party individuals.*`

Therefore, there is no reason to refuse the collection of data without demanding the consents of third parties.

9- Collecting data is necessary for the contractual fulfilment. The registrant gives extensive authority to the third party as the Admin-C and/or the Tech-C. They accept this role in order to perform an employment contact regarding the terms of IT services.

10- The applicant would like to explain and prove that the applicant has taken the necessary measures to ensure that the WHOIS is published in accordance with the GDPR. The data related to the Admin–C and the Tech-C shall not be open to the public without permission in accordance with temporary specification. (it will be analysed in section 4.2.)

11- If the court reaches the conclusion that the consequences of this procedure depend on the interpretation of some related articles of the GDPR, the court should ask these possible questions and refer the case to the European Court of Justice for preliminary ruling under Article 267 TFEU.

### 4.1.4.The Refusal of the ICANN`s Appeal of the Appellate Court of Cologne

ICANN, the applicant's appeal against the decision of the regional court of Bonn has been rejected on the 1st of August in 2018 by the 19th Civil Senate of the appeal court of Cologne. [110] The grounds of this decision are:

1- The court held that the applicant aims at a regulatory injunction. The main claim is solely claimed by the applicant on the basis of its statements and not based on the content.

2- The applicant has not proved that it is necessary to take preliminary measures to prevent significant disadvantages. According to the applicant`s petition, providing temporary assistance is required in order to prevent irreparable harm, otherwise the data will be lost. This argument was not found convincing.

3- As it is stated by the regional court of Bonn, the data was not absolutely necessary for the purposes of the applicant. The data including the Tech-C and the Admin-C were collected voluntarily before the GDPR. It was not a requirement for any purpose of the applicant.

4- Regarding the injunction, the court held that based on abstract risk/harm, the injunction cannot be granted. On the other hand, the previous experiences of ICANN has showed that non-collection of the data did not cause abusive action, thus, the argument of ICANN in this case has conflicted the previous practise of ICANN.

5- The senate decided not to refer the case to the European Court of Justice, since it is decided that the dispute is not coming from the interpretation of the GDPR.

[110] 19th Civil Senate of Appellate Court of Cologne Order with the docket no: 19 W 32/18, ICANN v. EPAG Domain services GmbH, Court decision, 1 August 2018.

### 4.1.5. The Plea of Remonstrance of ICANN Against The Decision Of The Appeal Court Of Cologne

After the refusal of their plea, the ICANN has submitted the plea of remonstrance of ICANN in order to continue the immediate appeal process based on section 321 of the German code of civil procedure (ZPO) on the 17th of August 2018.[111] The grounds are:

1- The court of appeal surprisingly provided a different view on the basis of incorrect assumptions. Even the defendant admits that the defendant would have to stop selling domain name registrations under the RAA in the event of such a court order. The court has considered that the demanded injunction is a regulating injunction. The injunction will only require the defendant to stop what he does, this is the essence of the applicant`s demand in the injunction. Therefore, this demand should be considered as a cease and desist claim.

2- There is no abstract risk. Especially, the legitimate interests contained in the abusive practices in the present case are of high importance to justify a preliminary dispute of abstract dangers.

3- The urgency requirement for granting an injunction for cease and desist is less strict than performance injunction. When the requirements of cease and desist injunction are analysed, the contractual obligation of the defendant was not questioned. A party can always ask for injunction in order to prevent further breach of a contract.

### 4.1.6 The Refusal of Plea Of Remonstrance by the Appellate Court of Cologne

The court rejected the plea of remonstrance on the 3rd of September 2018[112]. In order to avoid the repetition of the same grounds, it can be stated that the appellate court of cologne has rejected the plea of remonstrance based on the same grounds that are analysed in the decision of the regional court of Bonn in section 4.1.2. of chapter 4.

### 4.1.7. The Brief Evaluation of The Cases

In this section, the important points in the arguments of ICANN and the grounds of the decision will be explained according to my opinion.

First of all, the demand of ICANN is an injunction. Therefore, ICANN demands an injunction on the basis of the breach of the contract, since the registrar company does not share the personal data in order to comply with the GDPR. Actually, the court found that the claim of irreparable harm is abstract. However, if the plaintiff claims a potential violation rather than a solid example, irreparable damage assumption should be applied[113]. On the other hand, ICANN`s previous business model, namely a proxy and privacy service, was the main reason in rejecting the injunction. With the proxy and privacy services, data subjects have the right to hide their personal data on WHOIS. In addition to ICANN`s previous services, it also shows that there is no urgent need in

[111] Plea of Remonstrance of ICANN, Appellate Court of Cologne 19th. Senate for Civil Matters, August 17, 2018.
<https://www.icann.org/en/system/files/files/litigation-icann-v-epag-icann-plea-remonstrance-redacted-17aug18-en.pdf> (Consulting in 1 April 2019)
[112] 19th Civil Senate of Appellate Court of Cologne Order (n 10)
[113] David McGowan, Irreparable Harm, *Lewis & Clark L.* Rev., 2010, 14, pp. 577-596.

sharing personal data for WHOIS. Therefore, the court held that the claim of irreparable harm is found insubstantial.

In order to explain ICANN`s legitimate interest, ICANN showed a trademark system which provides unlimited online access to anyone. The idea of this openness is related to providing a research opportunity for an effective IP protection. The court did not explain why this argument was not considered. Perhaps, the reason is that the disputes on domain names do not always have to be related to trademarks, since, firstly, the disputes can exist due to a conflict of the company names rather than trademarks. Secondly, two different companies may want to use the same domain name in different sectors. For instance `ORANGE` is a domain name (https://www.orange.com/en/home) and company name in the telecommunications sector.[114] `ORANGE` is also being used as a domain name (https://www.orangecorporatefinance.nl/en/) by a different company in the finance sector.[115] In this case, companies may negotiate about the usage of domain names regardless their trademark registrations (since both have the trademark registrations in different classes). Therefore, domain name disputes might not be evaluated as a matter of intellectual property rights under certain circumstances. In this case a balance test is required in order to see whether the legitimate interest is to protect property rights or not.

As it is seen in the arguments in the court cases, the ICANN has argued that their new project, namely `temporary specification` gives the opportunity to be in compliance with the GDPR. However, the ICANN has failed four times in convincing the German courts about the effectiveness of `temporary specification` due to lacks of clear legitimate interest. In order to understand what ICANN has done wrong, in the next section, the new project of ICANN, temporary specification, will be analysed.

## 4.2 Temporary Specification

### 4.2.1 Background

In 2017, the ICANN hired a European law firm called Hamilton Advokatbyrå based on Stockholm, Sweden in order to get an independent legal support regarding the service of WHOIS[116]. The law firm has prepared a well-founded memorandum that consists of three parts. The following tools have been advised in the memorandum;

1- Implementing a layered access model which is an interim solution for the data processing for WHOIS.

[114] Orange is the largest providers of mobile and internet service operators and corporate telecommunication services in Europe and Africa. <https://www.orange.com/en/Group/Key-facts/Discover-Orange-s-key-facts> (Consulted in 13 May 2019)

[115] Sarah Bird, Trademark Law and Domain Names: ACPA or UDRP?, 2010. < https://moz.com/blog/trademark-law-and-domain-names-acpa-or-udrp> (Consulted in 13 May 2019)

[116] Hamilton GDPR Memorandum part 3, ICANN and Thomas Nygren and Pontus Stenbeck, Hamilton Advokatbyrå, 21 December 2017. <https://www.icann.org/en/system/files/files/gdpr-memorandum-part3-21dec17-en.pdf> (Consulted in 9 April 2019)

2- Informal dialogue with the Article 29 Working Party in order to continue to explore the possibility of the data usage publicly.

3- Data protection impact assessment (hereinafter DPIA) needs to be submitted to a EU members in order to be sure the compliance with the GDPR.

Given the advices above, on 12th of January 2018, ICANN released three proposed interim models in order to be compliant with the GDPR.[117] The ICANN opened these three models to advance community discussion in order to settle on a final compliance model. In this regard, `proposed interim model for GDPR compliance- summary description`[118] on 28th of February 2018 and `interim model for compliance with ICANN agreement and policies in relation to European Union`s GDPR- working draft for continued discussion`[119] on 8th of March 2018 are published.

These publications were analysed by Article 29 Working Party[120] (hereinafter WP29). According to the letter of WP29 on 11th of April 2018[121], it is announced that;

1. the interim model that includes `layer access`, `accreditation program` and `anonymized mail` have been found positive and effective.

2. it is emphasized that the importance of clear identification of `legitimate interest` in accordance with the requirements of GDPR. Therefore, the WP29 called the ICANN to reconsider the existing definition of `legitimate interest` in the light of the GDPR.

3. WP29 has warned that ICANN should not combine its own objectives with the interest of the third parties or the legal justification for a particular situation.

4. WP29 wants to emphasize that although a particular processing may serve various purposes, each individual objective can be justified by reference to a legal basis.

5. WP29 encouraged ICANN to make binding contractual commitments as it is suggested in final interim model.

---

[117] Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation – For Discussion, ICANN, 12 January 2018 <https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf> (Consulted in 14 April 2019)

[118] Proposed Interim Model for GDPR Compliance-- Summary Description, The "Calzone Model", ICANN, 28 February 2018. <https://www.icann.org/en/system/files/files/proposed-interim-model-gdpr-compliance-summary-description-28feb18-en.pdf> (Consulted in 14 April 2019)

[119] Interim Model for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation – working draft for continued discussion, The "Cookbook", ICANN, 8 March 2018. <https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf> (Consulted in 14 April 2019)

[120] The Article 29 working party is the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25th of May 2018. <https://edpb.europa.eu/our-work-tools/article-29-working-party_en> (Consulted in 16 April 2019)

[121] The letter from Article 29 Data Protection Working Party to ICANN regarding WHOIS directories and services, 11 April 2018.<https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf> (Consulted in 16 April 2019)

6. WP29 emphasized that ICANN still needs to introduce technical (including appropriate logging and auditing mechanism) and organisational safeguards in order to provide the safety of data.

7. In the final interim model, the period of the data retention is 2 years. ICANN needs to prove the necessity of this period in order to avoid the conflict of storage limitation principle of the GDPR.

8. ICANN needs to focus on the requirements of the international data transfers that comes with the GDPR, since the ICANN is domiciled in the USA.

After this letter, ICANN and WP29 had a meeting in Brussels on 23rd of April 2018.[122] Following this meeting, ICANN has addressed many questions to WP29 by sending another letter on 10th of May 2018[123]. WP29 has answered these questions on 5th of July 2018 by taking into the account temporary specification adopted on 17th of May 2018. The outcomes of the related questions and answers will be analysed together here below[124];

1- The European Data Protection Board (hereinafter EDPB) expected that ICANN improves a WHOIS model that provides legitimate uses of the concern parties such as law enforcement by providing limited data disclosure publicly.

2- The ICANN states many activities in order to persuade EDPB about the legitimate interests of ICANN. These are `maintaining the effectiveness of the gTLD registration system`, `promoting consumer trust`, `malicious abuse issues`, `protection of IPs ` and so on. Nevertheless, EDPB is of the opinion that a clear distinction must be maintained between the relevant objectives pursued by the various stakeholders involved in the WHOIS context.

3- A clear definition of the specific objectives pursued by ICANN cannot exclude the subsequent disclosure of personal data to third parties for their own interests and purposes from the requirements of GDPR.

4- In principle, the EDPB considers that the registrant should not be obliged to provide personal data identifying individual employees who perform administrative or technical functions on behalf of the registrant. Therefore, in the registration process, it should be clear that the registrant can choose the same person as registrant as technical and administrative contact or the registrant can provide a contact information that is not identifiable directly.

5- It is clear that the GDPR is not applying to legal person. However the fact that a registrant is a legal person does not justify the unrestricted publication of personal data

[122] https://www.icann.org/news/announcement-2018-04-12-en
[123] The letter from ICANN to Article 29 Working party, 10 May 2018 <https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-10may18-en.pdf> (Consulted in 16 April 2019)
[124] The European Data Protection Board`s letter to ICANN, 5 July 2018 <https://edpb.europa.eu/sites/edpb/files/files/news/icann_letter_en.pdf> (Consulted in 16 April 2019)

relating to natural persons working in or responsible for that institution, such as real persons managing the administrative or technical issues on behalf of the registrant.

6- Regarding to logging and auditing mechanism, the EDPB considers that an appropriate logging mechanism should be adopted to record any access to non-public personal data if it is not prohibited by the national law.

7- The EDPB reiterates ICANN`s request to review the recommended two years retention period and asked for a clear justification to retain personal data for this period.

After the legal advices, the discussions and the letters, the ICANN has accepted that they do not have overridden legitimate interest in making the data available to the public. In line with the goal of complying with GDPR, `temporary specification` is adopted in order to keep WHOIS effective as much as possible, while it restricts the processing of the personal data. As it is seen in lawsuits in Germany, ICANN itself has not found a mechanism in balancing the lawful interests of the parties in order to reach a lawful data processing under the GDPR. It does not explain a clear aim with the purpose of UDRP. Therefore, ICANN and Generic Name Supporting Organization (hereinafter GNSO) announced a new update of `temporary specification` called `Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process on 19th of February 2019. [125] (hereinafter Final Report of the Temporary Specification.)

### 4.2.2. What is new in `the updated version of temporary specification`?

In order to be in compliance with GDPR, on 17th of May 2018 ICANN decided to adopt ``temporary specifications`` which updates RAAs.[126] It is called `temporary`, since it is regulated for one year and the ICANN board must affirm it every 90 days.[127] However, temporary specification will be valid until 25th of May 2019. Whether temporary specification will be ICANN`s consensus policy or whether some modifications are required in temporary specification has been announced recently in Final report of the temporary specification.

Temporary specification will stay as an important source, since ICANN points out to the date of 29th of February 2020 as a target in initial implementation plan. Between for the gap between 25th of May 2019 and 29th of February 2020, the registrars must continue to comply with this gTLD Registration Data Policy or continue to take measures which consistent with `temporary specification`.[128]

In this section, ICANN`s steps in regulating the new policy for the efficiency of UDPR will be analysed.

---

[125] Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process, ICANN, 20 February 2019 <https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf> (Consulted in 19 April 2019)

[126] ICANN, Bylaws for Internet Corporation for Assigned Names and Numbers, § 1.1(a)(i) <https://www.icann.org/resources/pages/governance/bylaws-en/#article1> (Consulted in 19 April 2019)

[127] Summary of the Temporary Specification for gTLD Registration Data, ICANN, 6 June 2018. <https://www.icann.org/en/system/files/files/presentation-gtld-registration-data-temp-spec-06jun18-en.pdf> (Consulted in 19 April 2019)

[128] Id., p. 15.

#### 4.2.2.1. The Reasonable Access of IPR holders

According to section 4 regarding `access to non-public registration data`, registrars and registry operators must provide reasonable access to the third parties based on their legitimate interest which override fundamental rights of data subject.[129]

The reasonable access needs 3 elements to be fulfilled. These are;

i. The purpose limitation,
ii. Overriding legitimate interests compared to the privacy of the data subjects,
iii. The data minimisation principle.

First of all, the purpose limitation is an important steps in order to justify the access which basically violates the privacy rights of the data subject. Regarding the UDRP, the ICANN proposal outlines a more specific objective definition of WHOIS, which includes providing a credible mechanism for law enforcements needs. According to Annex D of the Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process[130], ICANN stated 7 different types of purpose regarding to the data processing and the sixth purpose clarifies that UDRP as a dispute solution is a purpose of the data processing. Moreover, the advantage of the data disclosure for UDRP has been clearly identified;

> `*The provision of this data to the complainant is important to help ensure due process for the registrant: it allows the complainant to withdraw a URS/UDRP claim where it becomes clear from the identity of the registrant that they have a right or legitimate interest to use the name, or that they have not registered the name in bad faith. It also enables, in some circumstances, requests to consolidate related claims, which has cost-saving benefits for all parties. In addition, the provision of this information to complainants supports case settlement (roughly 20% of cases) saving all parties time and expense*.`

Second, if you are the third party who has a legitimate interest in obtaining the data, you may contact the registrar and they have to respond within a reasonable time. First, a `Reasonable Request for Lawful Disclosure` should be applied by the third parties.[131] It does not mean that registrars have to disclose the data. The registrars shall evaluate each request on the legal basis of the GDPR. According to the recommendation with number 18 of Final report of the temporary specification[132], the minimum information required for the reasonable request for lawful data disclosure is that; identification and the information of the requestor, the justification of the request, confirmation that the request was made in good faith, the list of the requested data and an explanation about

[129] Temporary Specification for gTLD Registration Data, ICANN Board Resolutions, 17 May 2018. <https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-en.pdf> (Consulted in 19 April 2019)
[130] *Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process, Annex D* (n 125)
[131] Id., p. 18.
[132] Ibid.

why the data is limited to the need (data minimization principle[133]) and finally a contract for the legal data processing received in response to the request.

Regarding timeline and criteria for registrar and registry operator responses, in the 18th recommendation[134], it can be summarised under the following points;

- It should be acknowledged a data disclosure request without undue delay (not more than 2 business day starting from the day when the request is received). The time for response is maximum 30 days. However, if there is an extra ordinary circumstances such as high number of general requests. It also recommended that a specific deadline needs to be set for an urgent request.

- Decisions regarding the disclosure should be based on rationale grounds and the decision should include analysis or explanation of how the balancing test is applied.

It is debateable that all registrars companies are ready for these legitimate interest assessments. For instance, GoDaddy and Endurance International Group which is a web hosting company that has acquired numerous web hosting companies[135] stated that they have already been working with Data Protection Officers (hereinafter DPOs).[136] Regarding compliance with legal, regulatory and law enforcement requests, Godaddy have announced that they will disclosure the data which is necessary for a legal respond and claim to the government or third parties. [137] However, small companies have no announcement yet in this matter.

#### 4.2.2.2. Anonymized Email Address

To reach a balance between the privacy right and right to an effective remedy, according to Tara M. Aaron[138]:

> ``*another small light still shines through the privacy curtain, namely an anonymized email address.*``

In the event of non-consent , temporary specification still makes the communication by anonymous contact details. In section 2.5. of the temporary specification[139], the provisions enables an anonymized communication with the third parties if it is necessary. According to section 2.5.1.`*Registrar MUST provide an email address or a web form to facilitate email communication with the relevant contact, but MUST NOT identify the contact email address or the contact itself.*`

---

[133] According to Article 5 1(C), the meaning of data minimization is collecting adequate, relevant data which is limited to the purpose of the data processing.
[134] Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process, EPDP Team Recommendation 18 (n 125).
[135] Bluehost, Hostgator, BuyDomains are the examples of brands of Endurance International Group. <https://www.endurance.com/our-brands> (Consulted in 22 April 2019)
[136] https://uk.godaddy.com/legal/agreements/privacy-policy?pageid=privacy
[137] See Compliance with legal, regulatory and law enforcement requests.part, https://uk.godaddy.com/legal/agreements/privacy-policy?pageid=privacy
[138] Tara M. Aaron, Availability of WHOIS Information after the GDPR - Is It Time to Panic?, *The Law Journal of The International Trademark Association*, Vol. 108 No. 6., 2018, pp. 1129- 1142.
[139] *Final Temporary Specification for gTLD Registration Data, Appendix A* (n 125).

According to my opinion, whether anonymized email address provides a solution is questionable. Since, if a trademark owner contacts with a domain name owner over this system regarding a possible UDRP, the domain name owner can easily give the wrong information. For instance, as a reason of holding a domain name, she can state that she has a registered trademark in a country. Without the data, it is not possible to control whether the domain has a registered trademark. At this point, the trademark owner has no option apart from trusting what have been said to her. The trademark owner has no chance to prove that the domain name owner has no right or legitimate interest in respect of the domain name. Therefore, the trademark owner is not going to apply for a UDPR. In addition to this, when a trademark owner contacts the registrant by an anonymized email, it is not possible to determine whether this email has been received unless she receives a reply.[140] Ultimately, anonymized way of communication does not provide an effective solution.

#### 4.2.2.3. The Safeguards For International Data Transfers

Given the fact that ICANN is domiciled in the USA, the data transfers and processing should be compliance in the regulation for international data transfer. According to Article 45 of GDPR, the data transfer should be on the basis of adequacy decision which confirms that the country where the data will be sent to has adequate safeguards in data protection. At this point, we are coming back to the dilemma of the data protection in regard to the EU-US privacy shield. According to Commission Implementing Decision (EU) 2016/1250 of 12th July 2016, it has approved that the US law is compliance with the cross-border data transfer requirements under the GDPR. While the Schrems 2 case is pending against the privacy shield before CJEU, according to European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield[141], the privacy shield does not provide adequate safeguards in protecting individual`s right. The despite the fact that the implementation on the privacy shield is affirmative, the EDPB announced that there are still concerns about the implementation of the privacy shield on 24th of January 2019.[142] Consequently, the future of the privacy shield is not clear. Therefore, ICANN needs to prepare a plan in the event of non-adequacy decision in order to continue the data flow from European countries to the USA.

According to the Article 46 of GDPR:

> *`In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only*

[140] WHOIS Challenges: A Toolkit for Intellectual Property Professionals, the WHOIS/RDS Subcommittee of the Internet Committee, INTA, 2018. <https://www.inta.org/Advocacy/Documents/2018/WHOIS%20Challenges%20A%20Toolkit%20for%20Intellectual%20Property%20Professionals.pdf> (Consulted in 22 April 2019)

[141] European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, European Parliament, 5 July 2018. <http://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.pdf> (Consulted in 22 April 2019)

[142] EU - U.S. Privacy Shield - Second Annual Joint Review, European Data Protection Board, 22 January 2019 https://edpb.europa.eu/sites/edpb/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf? (Consulted in 22 April 2019)

*if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.`*

In parallel with the abovementioned article, ICANN has regulated that appropriate technical and organizational measures should be applied in order to provide a security level in accordance with the risk of data processing by taking into consideration the state of the art technology, the costs, the scope, objectives of the transaction and the risk of the transaction.[143] These safeguards are not limited with section 3.8. and have been regulated widely. However, ICANN have not announced any solid steps regarding the safeguards for international data transfers such as certified system or code of conduct regarding the data collecting process.

### 4.3 The Regulation for `.eu` Domain Names

`.eu` is the country code top level domain of the European Union. The purpose of `.eu` is to enhance European Union identity by respecting multilingualism and people`s privacy and security.[144] The system of EURid is in compliance with the GDPR, thus, it might be a great example for ICANN. In this section, the system of EURid will be analysed. However, it is important to keep in mind that EURid does not provide any system for cross-border data flow, since ccTLD is only for the European Union.

First of all, EURid regulated itself as a controller and registrar companies become processors[145]. This might be very practical, since each registrar company would not have to hire a DPO separately. All the data assessments will be controlled and evaluated by one hand. In this way, ICANN also prevents the fragmentation in domain name law. Today, in the ICANN system is not clear who the controller is and who the processor is. Secondly, EURid stores the personal data in Europe.[146] Apparently ICANN will suffer due to the possible cancellation of the EU-US privacy shield. This dilemma does not seem like it is going to be solved within a short period due to the differences between US and EU approaches regarding data protection law. Therefore, storing the data in Europe in order to avoid cross-border data flow from Europe to USA (the section 4.2.2.3. of chapter 4) might be a solution. The data disclosure for an UDRP might then require a typical and not cross border data process as is mentioned in Article 4 of the EURid registrar agreement.[147] However, that would be a partial solution, since the .eu domain name is only available for the countries in Europe excluding the United Kingdom.[148] However ICANN needs more of a inclusionary system in order to reach a uniform system. Therefore, the final and certain solution for ICANN is laying down in a strong and safe mechanism where the balance between parties is provided. Thirdly,

[143] *Final Temporary Specification for gTLD Registration Data, Appendix C: Data Processing Requirements, Section 3.8* (n 125)
[144] Regulation (EU) 2019/517 of the European Parliament and of the Council of 19 March 2019 on the implementation and functioning of the .eu top-level domain name and amending and repealing Regulation (EC) No 733/2002 and repealing Commission Regulation (EC) No 874/2004
[145] https://eurid.eu/en/register-a-eu-domain/gdpr/
[146] Ibid.
[147] EURid registrar agreement, Version 7.1, 6 May 2019, <https://eurid.eu/d/5281306/Registrar_agreement_en_stamped.pdf> (Consulted in 17 May 2019)
[148] https://eurid.eu/en/register-a-eu-domain/brexit-notice/

EURid provides limited online research on WHOIS. Only the language and an e-mail address (kind of anonymised e-mail address) of the registrant are available on WHOIS. The availability of language might be helpful in determining the language of a possible UDRP. Fourthly, a party who has legitimate interest may demand extra data by completing the request form. The request form is similar with the `Reasonable Request for Lawful Disclosure` in the temporary specification of ICANN. EURid also expect the third parties to explain their legitimate interest, why and where the data is intended to be used.[149] Finally, paragraph 23 of the regulation[150] requires an independent audit for the registry (EURid) in order to assure effectiveness of EURid.

Consequently, it can be said that there are substantial similarities between the updated temporary specification of ICANN and the regulation for `.eu` domains. However, there are also some main differences. One main difference is that ICANN needs to establish a mechanism for cross-border data flow, thus, it is important to have a flexible mechanism in terms of compatibility with various national laws. Another difference is that EURid is a registry[151] and controller in terms of data protection law. However, in the mechanism of ICANN, registrars should evaluate each request for the lawful disclosure. According to my opinion, this is the most important drawback of ICANN`s system, since there is no main body to control registrars` activities. In addition to this, the wide discretionary power of registrar companies constitutes an impediment in harmonisation of the data disclosure request process.

[149] https://eurid.eu/en/register-a-eu-domain/domain-name-disputes/

[150] Paragraph 23 of Regulation (EU) 2019/517 of the European Parliament and of the Council of 19 March 2019 on the implementation and functioning of the .eu top-level domain name and amending and repealing Regulation (EC) No 733/2002 and repealing Commission Regulation (EC) No 874/2004.

[151] Registrar Agreement, EURid, version of 6 May 2019, <https://eurid.eu/d/5281306/Registrar_agreement_en_stamped.pdf> (consulted in 31 May 2019)

# Conclusion

In this thesis, my aim is to explain the effects of the GDPR on the UDRP and to figure out the possible solutions for the problem that comes with the GDPR. After the GDPR, the WHOIS database which is a main step in starting a UDRP process is no longer available online. Inaccessibility of WHOIS undermines the UDRP process, since IPRs holders cannot research about the requirements of the UDRP policy. There is a conflict between right for an effective remedy of trademark owners (Article 47 of Charter and Article 13 of ECHR), right to protection of property (Protocol 1, Article 1) and privacy right of the domain name owners (Article 7 and 8 of the Charter, Article 8 of ECHR).

To begin with the current situation, the digital market is showing the significant growth, the number of domain names has been rising steadily. Thousands domain names from hundreds countries meet in the same platform, namely the internet. Therefore, the risk of being conflicted with a trademark in domain registration is getting very high on the internet due to the fact that non harmonic structure of domain registration. The disadvantage of the internet as a platform that enables elusive IP infringements was used to be stopped by the UDRP process. However in post-GDPR world, UDPR may lose its effectiveness, despite the fact that it was a great example in combating with the technologic turbulence.

The GDPR is at risk of being the `law of everything` with the aim of delivering the highest legal protection in all circumstances.[152] Anonymity has the full command of the internet rather than the real aim of the GDPR. The rising problem of anonymity on the internet is getting a challenge for law enforcements parties. For instance, in order to take legal action, it is needed to know the name, address of the defendant party, which is not possible in most cases of trademark violation in the internet. Most of time, even if lawyers or trademark attorneys detect an infringement on the website where the infringement occurs, reaching the necessary data to initiate legal process is a challenging step for the law enforcement parties. Without knowing potential respondents in an UDPR case, it is hard to advise any legal steps, since attorneys need to prove bad faith of the respondent in holding a disputed domain name.

While figuring out solutions, It is important to see how ICANN`s position is different. ICANN should not be considered as typical private companies that avoid the GDPR compliance such as Google or Facebook. [153] On the other hand, It is also true that ICANN takes advantages of inevitable technological developments to avoid basic compliance with right to privacy.[154] Besides the uniqueness of ICANN, the UDRP has also a special place among the other ways of arbitration. Since, the UDPR has remarkable success in the digital era while online infringement becomes problematic

[152] Nadezhda Purtova, The law of everything. Broad concept of personal data and future of EU data protection law, *Law Innovation And Technology*, 2018, Vol 10, No. 1, 40–81

[153] Stephanie E. Perrin, The Struggle for WHOIS Privacy: Understanding the Standoff Between ICANN and the World's Data Protection Authorities (doctoral dissertation), Faculty of Information University of Toronto, 2018, pp 242.
< https://tspace.library.utoronto.ca/handle/1807/89738> (consulted 6 May 2019)

[154] Ibid.

due to the lack of an effective national law system (as it is mentioned in chapter 2). Consequently, according to my opinion the problem regarding the WHOIS database should not be evaluated only as a business model of ICANN, it should be considered that the UDRP process also includes public interest in itself[155]. Effectiveness of WHOIS is very important for IPR holders and the end users (in the event of the deceptive counterfeiting).

Given this unique structure of ICANN, the legitimate interest of the lawsuits of ICANN tried to be explained before the German courts, since the legitimate interest of ICANN was the strongest argument that might be claimed in data processing in this case. I think, due to the previous experience of ICANN (privacy and proxy service), this argument did not get the attention as it deserved in the lawsuit. The German court evaluated the previous practice called privacy service (see section 3.2.2. of chapter 4) in a punitive way. The conflict between what ICANN did and what ICANN wants to do after the GDPR became a very big dilemma to the detriment of ICANN. Given the fact of the legitimate interest of ICANN`s activities, I am of the opinion that the legitimate interest of ICANN should have been accepted despite the wrong practice of ICANN in the past.

Despite abovementioned lawsuits and the temporary specification, ICANN failed to convince the court of the compliance with the GDPR. From this point on, the focus will be on what ICANN can do more according to my opinion. First of all, as it is seen in the regulation for the `.eu` domain, ICANN may establish a new system where ICANN is a registry and controller. The legal assessments regarding the data disclosure requests should be handled by one main body, since in the current system, registrar companies have been developing their own rules. This causes fragmentation in the domain management system in domain name law, since different privacy teams or DPOs in different registrar companies may make different decisions in similar cases. In the end, it may cause a less trustful system of ICANN. On the other hand, registrar companies may be more likely to reject the request for lawful data processing in order to avoid the possible fine in the event of a violation of the GDPR. This may disable the effectiveness of WHOIS. Therefore, evaluation for the request for the lawful processing should be carried out by ICANN in cooperation with the registrar companies. ICANN needs to prepare an independent agreement between registrants and itself. In this way, ICANN may create a new ground for lawful data processing (paragraph (b) of Article 6). The whole discussion shows that ICANN needs to establish a data protection team which contains DPOs in order to deal with the requests for lawful data processing. Given the fact that besides European countries, other countries have or will have data protection regulations, this privacy team will play a fundamental role in the effectiveness of WHOIS across the world.

[155] Simone Vezzani, ICANN's New Generic Top-Level Domain Names Dispute Resolution Procedure Viewed Against the Protection of the Public Interest of the Internet Community: Litigation Regarding Health-Related Strings, *The Law and Practice of International Courts and Tribunals 13*, 2014, pp. 306–346

These abovementioned steps might be taken over a long period of time. Within short time, ICANN may lead its panellists to reinterpret the provision of the bad faith in UDRPs. In addition to this, the panellists need to be encouraged to take much more initiative in deciding being in bad faith. However, theoretically, the rebuttable presumption of being in good faith in civil code will preclude the flexible way of interpreting `bad faith` for UDPR process in post-GDPR world.

# Bibliography

## Books


- Bettinger, T. and Waddell, A., *Domain Name Law and Practice An International Handbook*, Oxford University Press, Oxford, 2015 p. 140.

- Bruen, G. O., *WHOIS Running the Internet: Protocol, Policy, and Privacy*, John Wiley & Sons Inc, Hoboken New Jersey, 2015, p. 207.

- Keith, M., *Private Rights and Public Problems : The Global Economics of Intellectual Property in the 21st Century*, Peterson Institute press 2012, Washington DC, 2012.

- Piers, M. and Aschauer, C., *Arbitration in the Digital Age: The Brave New World of Arbitration*, Cambridge University Press, Cambridge, 25 Jan 2018.


## Handbooks


- Protecting the right to respect for private and family life under the European Convention on Human Rights Council of Europe human rights handbooks, Council of Europe Strasbourg, 2012. <https://www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf>(Consulted in 8 May 2019)

- Handbook on European data protection law 2018 Edition, European Union Agency for Fundamental Rights and Council of Europe, European Court of Human Rights, Council of Europe, European Data Protection Supervisor, 2018. <https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf> (Consulted in 8 May 2019)


## Articles


- Aaron, T. M., Availability of WHOIS Information after the GDPR - Is It Time to Panic?, *The Law Journal of The International Trademark Association*, Vol. 108 No. 6., 2018, pp. 1129- 1142.

- Bartlett, A. and Morgan, A., Osborne Clarke, Enforcement of judgement and arbitral awards in the UK overview, *Enforcement of Judgements and Arbitral Awards in Commercial Matters Global Guide 2018*, 2018, pp 1-16.

- Bender, R. G., Arbitration—An Ideal Way to Resolve High-Tech Industry Disputes, *The Dispute resolution Journal* November 2010 / January 2011, Vol.65, No. 4 pp. 1- 9.

- Birkbeck, C. D., The Politics of Intellectual Property Reform in Developing Countries: The Relevance of the World Intellectual Property Organization, *Oxford University Press,* 2009, pp. 111-133.

- Brkan, M., In search of the concept of essence of EU fundamental rights through the prism of data privacy, *Maastricht Faculty of Law Working Paper,* 2017, Vol 1, pp. 1-29.

- Cheryl H. Agris, Stephen P. Gilbert, Charles E. Miller and Sherman Kahn, The Benefits of Mediation and Arbitration for Dispute Resolution in Intellectual Property Law, *New York Dispute Resolution Lawyer*, 2011, Vol. 4 No. 2 pp. 61-65.

- Cremades, B. M. and Cortes, R., The Principle of Confidentiality in Arbitration: A Necessary Crisis, *Journal of Arbitration Studies,* 2013, vol 23 No 3, page 25-38.

- Kostic, B. and Penagos, E. V., The freely given consent and the "bundling" provision under the GDPR, *AFL*, 2017, 4, pp. 217-222.

- Lindenthal, T., Valuable Words: The Price Dynamics of Internet Domain Names, *Journal Of The Association For Information Science And Technology, Massachusetts Institute of Technology*, 2014 65(5), pp . 869–881.

- Massoud, M. F., *International Arbitration and Judicial Politics in Authoritarian States Law Soc Inq*, 2014, vol 39, issue 1, pp 1-30.

- McGowan, D. Irreparable Harm, *Lewis & Clark L.* Rev., 2010, 14, pp. 577-596.

- Mueller, M. L., The battle over Internet domain names. Global or national TLDs? *Telecommunication Policy,* 1998, Vol. 22, No. 2, pp. 89—107.

- Nzololo, M. and Makany, R. A., Economic Analysis Of Non-Deceptive Counterfeiting In Congo *Int.J.Eco.Res.*,2015, v6 i6, pp. 08 – 21.

- Purtova, N., The law of everything. Broad concept of personal data and future of EU data protection law, *Law Innovation And Technology*, 2018, Vol 10, No. 1, 40–81

- Renck, A.W., Kennzeichenrechte versus Domain Names-Eine Analyse der Rechtsprechung, *Neue Juristische Wochenschrift (NJW)*, 1999, 49, pp. 3587-3590.

- Woodard, E. C., The UDRP, ADR, and Arbitration: Using Proven Solutions to Address Perceived Problems with the UDRP, *Fordham Intellectual Property, Media and Entertainment Law Journal*, 2009, Vol 19, No 4, pp. 1170-1212.

➢ Vezzani, S., ICANN's New Generic Top-Level Domain Names Dispute Resolution Procedure Viewed Against the Protection of the Public Interest of the Internet Community: Litigation Regarding Health-Related Strings, *The Law and Practice of International Courts and Tribunals 13*, 2014, pp. 306–346.

➢ Zammit, J. P. and Hu, J., Arbitrating International Intellectual Property Disputes, *Dispute Resolution Journal*, November 2009/ January 2010, pp. 1-4.

➢ Zugelder, M. T., Flaherty, T. B. and Johnson, J. P., Legal issues associated with international Internet marketing, *International Marketing Review*, 2000, Vol. 17 Issue: 3, pp.253-271.

➢ Verma S., Kumar R., and Philip P.J., The Business of Counterfeit Drugs in India: A Critical Evaluation, *International Journal of Management and International Business Studies*, 2014, Volume 4, Number 2, pp. 141-148.

## Doctoral Dissertation

➢ Perrin, S. E., The Struggle for WHOIS Privacy: Understanding the Standoff Between ICANN and the World's Data Protection Authorities (doctoral dissertation), Faculty of Information University of Toronto, 2018, pp 242.

## Legislations and Policies

➢ Charter of Fundamental Rights of the European Union (adopted 18 December 2000, effective 1 December 2009) 2012/C 326/02 ('Charter')

➢ Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5

➢ European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14

➢ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

➢ Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

➢ Regulation (EU) 2019/517 Of The European Parliament And Of The Council of 19 March 2019 on the implementation and functioning of the .eu top-level domain name

and amending and repealing Regulation (EC) No 733/2002 and repealing Commission Regulation (EC) No 874/2004.

- ICANN, Bylaws For Internet Corporation For Assigned Names And Numbers, As amended 18 June 2018.

- Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") as approved by the ICANN board of directors on 30 October 2009.

## Jurisprudence

### 1. Decisions of the Court of Justice of the European Union and European Court of Justice

- CJEU, Productores de Música de España (Promusicae) v. Telefónica de España SAU [GC], C-275/06, 29 January 2008.

- ECtHR, S. And Marper v. The United Kingdom, Applications no. 30562/04 and 30566/04, 4 December 2008.

- CJEU, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen [GC], 9 November 2010.

### 2. Decisions of National Courts

- The Regional Court of Bonn the docket-no. 10 O 171/18, f Internet Corporation for Assigned Names and Numbers (ICANN) v. EPAG Domain services GmbH, Court Order In the preliminary injunction proceedings, 29 May 2018.

- 19th Civil Senate of Appellate Court of Cologne Order with the docket no: 19 W 32/18, ICANN v. EPAG Domain services GmbH, Court decision, 1 August 2018.

### 3. WIPO Cases

- WIPO Arbitration and Mediation Center, Panelist Torsten Bettinger, Stanworth Development Limited v. Dr. Ricardo Vasquez Case No D 2008-0943, Administrative Panel Decision, 20 August 2008.

- WIPO Arbitration and Mediation Center, Panelist Jeffrey M. Samuels, Pearson Education, Inc v. CTP Internacional; Private Registration at Directi Internet Solutions Pvt. Ltd. and <scottforesmanandcompany.com> Case No D 2009-0266, Administrative Panel Decision, 11 May 2009.

➢ WIPO Arbitration and Mediation Center, Panelist Haig Oghigian, AXA SA v. Value Domain Case No. D2009-1015, Administrative Panel Decision, 22 September 2009.

➢ WIPO Arbitration and Mediation Center, Panelist Luca Barbero, M/s Genpact Limited v. Contact Privacy Inc. / self, Case no D 2012-0307, Administrative Panel Decision, 10 April 2012.

➢ WIPO Arbitration and Mediation Center, Panelist Alvaro Loureiro Oliveira, Intesa Sanpaolo S.p.A. v. Croitoru Daniel Case D 2012- 1113, Administrative Panel Decision, 20 August 2012.

➢ WIPO Arbitration and Mediation Center, Panelist M. Scott Donahey, Alleghany Pharmacal Corporation v. Hair for Life case No D 2003-1045, Administrative Panel Decision, 26 February 2014.

➢ WIPO Arbitration and Mediation Center, Panelist Karen Fong, F. Hoffmann-La Roche AG v. Konayem Temirtassova, Tigran Movsisyan and the others case no D 2015-0984, Administrative Panel Decision, 7 September 2015.

➢ WIPO Arbitration and Mediation Center, Panelist Reyes Campello Estebaranz, Compagnie Générale des Etablissements Michelin v. Balticsea LLC, Case No. D 2017-0308, Administrative Panel Decision, 10 April 2017.

➢ WIPO Arbitration and Mediation Center, Panelist Roberto Bianch, Bayerische Motoren Werke AG (BMW) v. Balog Sebastian, Administrative Panel Decision, 18 September 2017, Case No. D2017-1407.

➢ WIPO Arbitration and Mediation Center, Panelist Louis-Bernard Buchman, Star Stable Entertainment AB v. Dawid Olszewski, Administrative Panel Decision, 27 July 2018, Case No. D2018-1293.

## Reports

➢ 2017 Situation Report on Counterfeiting and Piracy in the European Union, A joint project between Europol and the European Union Intellectual Property Office, 2017<https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union> (consulted in 5 December 2018)

➢ The Domain Name Industry Brief, The Verisign Domain Report, 2018, <https://www.verisign.com/assets/domain-name-report-Q32018.pdf> (Consulted in 11 January 2019)

➢ Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process, ICANN, 20 February 2019 <https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf> (Consulted in 19 April 2019)

## Other Documents

### 1. Other Documents Issued By ICANN

➢ Temporary Specification for gTLD Registration Data, Annex: Important Issues for Further Community Action. More details in the Section 2.5.1 of Appendix A, ICANN, 2018 <https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#appendixA> (Consulted in 5 November 2018)

➢ General Data Protection Regulation (GDPR) & WHOIS at ICANN, ICANN, Savenaca Vocea APNIC 46, Noumea 11.09.2018 <https://conference.apnic.net/46/assets/files/APNC402/GDPR-and-Whois-at-ICANN.pdf> (Consulted in 3 November 2019)

➢ Registrar Accreditation Agreement, 3.3 Public Access to Data on Registered Names<https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>(Consulted in 11 February 2019)

➢ Section 3.3. of 2013 Registrar Accreditation Agreement, ICANN, 17 September 2013 <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa> (Consulted in 22 April 2019)

➢ DNA Healthy Domain Initiative, Registry/ Registrar Healthy Practise, The Domain Name Association (The DNA), 8 February 2017. < http://www.thedna.org/wp-content/uploads/2017/02/DNA_Healthy_Practices_2017.pdf> (Consulted in 1 April 2019)

➢ GDPR Domain Industry Playbook, Association of the Internet Industry, Julia Garbaciok, Andreas Konrad, Martin Lose, Thomas Rickert, Jan Schlepper, Oliver Süme, 2017 < https://www.eco.de/wp-content/uploads/2017/12/20171208-DRAFT_eco_GDPR_Playbook.pdf> (Consulted in 29 May 2019)

➢ Hamilton GDPR Memorandum part 3, ICANN and Thomas Nygren and Pontus Stenbeck, Hamilton Advokatbyrå, 21 December 2017. <https://www.icann.org/en/system/files/files/gdpr-memorandum-part3-21dec17-en.pdf> (Consulted in 9 April 2019)

➢ Hamilton GDPR Memorandum part 1, Thomas Nygren and Pontus Stenbeck, Hamilton Advokatbyrå, 16 October 2017. < https://www.icann.org/en/system/files/files/gdpr-memorandum-part1-16oct17-en.pdf> (Consulted in 29 May 2019)

➢ Summary of the Temporary Specification for gTLD Registration Data, ICANN, 6 June 2018. <https://www.icann.org/en/system/files/files/presentation-gtld-registration-data-temp-spec-06jun18-en.pdf> (Consulted in 19 April 2019)

➢ Temporary Specification for gTLD Registration Data, ICANN Board Resolutions, 17 May 2018. <https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-en.pdf> (Consulted in 19 April 2019)

➢ Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation – For Discussion, ICANN, 12 January 2018 <https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf> (Consulted in 14 April 2019)

➢ Proposed Interim Model for GDPR Compliance-- Summary Description, The "Calzone Model", ICANN, 28 February 2018. <https://www.icann.org/en/system/files/files/proposed-interim-model-gdpr-compliance-summary-description-28feb18-en.pdf> (Consulted in 14 April 2019)

➢ Interim Model for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation – working draft for continued discussion, The "Cookbook", ICANN, 8 March 2018.<https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf> (Consulted in 14 April 2019)

## 2. Others Documents issued by other organizations

➢ A Study of Whois Privacy and Proxy Service Abuse, National Physical Laboratory, 2013.<https://gnso.icann.org/sites/default/files/filefield_41831/pp-abuse-study-20sep13-en.pdf> (Consulted in 11 May 2019)

➢ WHOIS Challenges: A Toolkit for Intellectual Property Professionals, INTA, 2015 <https://www.inta.org/Advocacy/Documents/2018/WHOIS%20Challenges%20A%20Toolkit%20for%20Intellectual%20Property%20Professionals.pdf> (consulted by 5 November 2018)

➢ WHOIS Challenges: A Toolkit for Intellectual Property Professionals, the WHOIS/RDS Subcommittee of the Internet Committee, INTA, 2018. <https://www.inta.org/Advocacy/Documents/2018/WHOIS%20Challenges%20A%20Toolkit%20for%20Intellectual%20Property%20Professionals.pdf> (Consulted in 22 April 2019)

➢ Arbitration as A Dispute-Solving Mechanism in Public Procurement: A Comparate View Between Peruvian and Spanish Systems, Alexandra Molina Dimitrijevich, <http://www.ippa.org/IPPC4/Proceedings/01ComparativeProcurement/Paper1-18.pdf> (Consulted in 15 November 2019)

➢ International Trademark Association, Addressing the Sale of Counterfeits on the Internet, INTA, 2017 <https://www.inta.org/Advocacy/Documents/2018/Addressing_the_Sale_of_Counterfeits_on_the_Internet_021518.pdf> (Consulted in 17 May 2019)

➢ China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy, United States International Trade Commission, 2011<https://www.usitc.gov/publications/332/pub4226.pdf> (Consulted in 8 January 2019).

➢ Measuring the magnitude of global counterfeiting: creation of a contemporary global measure of physical counterfeiting, US Chamber of Commerce, Washington DC, 2016. <https://www.uschamber.com/sites/default/files/documents/files/measuringthemagnitudeofglobalcounterfeiting.pdf> (Consulted in 9 January 2019)

➢ The Economic Effects of Counterfeiting and Piracy, A Review and Implications for Developing Countries, Policy Research Working Paper 7586, World Bank Group, Development Economics Vice Presidency Operations and Strategy Team, 2016. http://documents.worldbank.org/curated/en/909261467990967406/pdf/WPS7586.pdf> (Consulted in 11 January 2019)

➢ Joint Recommendation Concerning Provisions on the Protection of Marks, and Other Industrial Property Rights in Signs, on the Internet, adopted by the Assembly of the Paris Union for the Protection of Industrial Property and the General Assembly of the World Intellectual Property Organization (WIPO), 2001<https://www.wipo.int/edocs/pubdocs/en/wipo_pub_845.pdf> (Consulted in 11 February 2019)

➢ Internet Management, Prevalence of False Contact Information for Registered Domain Names, United States Government Accountability Office, 2005 < https://www.gao.gov/new.items/d06165.pdf> (Consulted in 11 February 2019)

➢ The letter from the attorney of FRL Registry B.V to ICANN,09.10.2017 <https://www.icann.org/en/system/files/correspondence/sprey-to-Marby-9oct17-en.pdf> (Consulted in 18 February 2019)

➢ Article 29 Data Protection Working Party letter to ICANN, 06 December 2017<https://www.icann.org/en/system/files/correspondence/falque-pierrotin-to-chalaby-marby-06Dec17-en.pdf>(Consulted in 8 May 2019)

➢ Opinion on the application of the necessity and proportionality concepts and data protection within the law enforcement sector, WP 211, Article 29 Data Protection Working Party, 2014. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf> (Consulted in 8 May 2019)

➢ WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Third Edition ("WIPO Overview 3.0"), WIPO, 2017 <https://wipo.int/amc/en/domains/search/overview3.0/#item36> (Consulted in 16 April 2019)

➢ A preliminary injunction demand of ICANN against EPAG Domain services GmbH before Regional Court of Bonn, 25 May 2018. <https://www.icann.org/en/system/files/files/litigation-icann-v-epag-request-prelim-injunction-redacted-25may18-en.pdf> (Consulted in 9 April 2019).

➢ The immediate Appeal Petition to Regional Court of Bonn 10th Civil Chamber, ICANN v. EPAG Domain services GmbH, 13 June 2018. <https://www.icann.org/en/system/files/files/litigation-icann-v-epag-immediate-appeal-redacted-13jun18-en.pdf> (Consulted in 15.05.2019).

➢ Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Article 29 Data Protection Working Party 17/EN WP 253, 3 October 2017. <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237> (Consulting in 5 April 2019)

➢ Opinion 03/2013 on purpose limitation, Article 29 Data Protection Working Party, 00569/13/EN WP 203, 2 April 2013. https://ec.europa.eu/justice/article29/documentation/opinionrecommendation/files/2013/wp203_en.pdf> (Consulting in 5 April 2019)

➢ Plea of Remonstrance of ICANN, Appellate Court of Cologne 19th. Senate for Civil Matters, August 17, 2018.<https://www.icann.org/en/system/files/files/litigation-icann-v-epag-icann-plea-remonstrance-redacted-17aug18-en.pdf> (Consulting in 1 April 2019)

➢ The letter from Article 29 Data Protection Working Party to ICANN regarding WHOIS directories and services, 11 April 2018.<https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf> (Consulted in 16 April 2019)

➢ The letter from ICANN to Article 29 Working party, 10 May 2018 <https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-10may18-en.pdf> (Consulted in 16 April 2019)

➢ The European Data Protection Board`s letter to ICANN, 5 July 2018 <https://edpb.europa.eu/sites/edpb/files/files/news/icann_letter_en.pdf> (Consulted in 16 April 2019)

➢ European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, European Parliament, 5 July 2018. <http://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.pdf> (Consulted in 22 April 2019)

➢ EU - U.S. Privacy Shield - Second Annual Joint Review, European Data Protection Board, 22 January 2019 https://edpb.europa.eu/sites/edpb/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf? (Consulted in 22 April 2019)

➢ EURid registrar agreement, Version 7.1, 6 May 2019, <https://eurid.eu/d/5281306/Registrar_agreement_en_stamped.pdf> (Consulted in 17 May 2019)

➢ Registrar Agreement, EURid, version of 6 May 2019, <https://eurid.eu/d/5281306/Registrar_agreement_en_stamped.pdf> (consulted in 31 May 2019)

### Websites and blogs

➢ Martin Scheinin, The Essence of Privacy and Varying Degrees of Intrusion, 2015 <https://verfassungsblog.de/the-essence-of-privacy-and-varying-degrees-of-intrusion-2/> (Consulted in 8 May 2019)

➢ Sarah Bird, Trademark Law and Domain Names: ACPA or UDRP?, 2010. < https://moz.com/blog/trademark-law-and-domain-names-acpa-or-udrp> (Consulted in 13 May 2019)

➢ Shraddha, Trademark issues, related to Internet Domain Names, 2018 <https://blog.ipleaders.in/trademark-issues-related-to-internet-domain-names/> (Consulted in 26 April 2019)

➢ ccTLD database contains links to ccTLD registration agreements, WHOIS services and alternative dispute resolution procedures <http://www.wipo.int/amc/en/domains/cctld_db/output.html> (Consulted in 2 May 2019)

➢ About .jp domains <https://uk.godaddy.com/help/about-jp-domains-20219> (Consulted in 2 March 2019)

➢ Rules for the Allocation of Domain Names Under the Israel Country Code Top Level Domain (".IL") <https://www.isoc.org.il/files/docs/ISOC-IL_Registration_Rules_v1.6_ENGLISH_-_18.12.2017.pdf> (Consulted in 2 March 2019)

➢ What is WHOIS data used for? <https://whois.icann.org/en/what-whois-data-used> (Consulted in 4 March 2019)

➢ GDPR explanation <https://eurid.eu/en/register-a-eu-domain/gdpr/> (Consulted in 4 May 2019)

➢ Data Privacy Statement of Denic <https://www.denic.de/en/about-denic/data-privacy-statement/> (Consulted in 4 May 2019)

➢ WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Original Edition <https://www.wipo.int/amc/en/domains/search/overview2.0/#39> (Consulted in 4 February 2019)

➢ Impact of Changes to Availability of WhoIs Data on the UDRP: WIPO Center Informal Q&A <https://wipo.int/amc/en/domains/gdpr/> , (Consulted in 1 May 2019)

➢ On WHOIS Privacy & Proxy Services <https://www.icann.org/news/blog/on-whois-privacy-proxy-services> (Consulted in 4 February 2019)

➢ https://thedna.org/what-is-the-domain-name-association/

➢ https://www.icann.org/news/announcement-2018-05-25-en

➢ https://www.icann.org/news/announcement-2018-04-12-en

➢ https://au.godaddy.com/help/gdpr-faq-27923

➢ https://in.godaddy.com/help/why-is-domains-by-proxy-no-longer-available-in-gdpr-affected-areas-27925