hamilton

MEMORANDUM

To	Internet Corporation for Assigned Names and Numbers
From	Thomas Nygren and Pontus Stenbeck, Hamilton Advokatbyrå
Date	21 December 2017 – DRAFT 3
Subject	gTLD Registration Directory Services and the GDPR - Part 3

1. BACKGROUND, SCOPE AND STRUCTURE

1.1 In its preparations for the entering into force of the EU General Data Protection Regulation 2016/679 (the "**GDPR**") on 25 May 2018, the Internet Corporation for Assigned Names and Numbers ("**ICANN**") has requested Hamilton Advokatbyrå to provide an independent assessment of the legal challenges that the GDPR will entail in relation to the registration directory services for generic top-level domains ("**gTLDs**"), commonly known as Whois, that is made available to the general public on the requirement of ICANN.

1.2 Our assignment focuses on the processing of data which ICANN currently requires registrars (accredited by ICANN) and registries (registry operators) to obtain from domain name registrants ("**Whois data**"), in particular personal data, which is being maintained by registrars and registries in different directories and made publicly available through so-called look-up tools (any services provided in relation to Whois data are herein jointly referred to as "**Whois services**"). Our analysis will primarily be based on the preferred option of ICANN for the Whois services to remain in their current state following the GDPR entering into force. For the avoidance of doubt, it should be noted that our analysis will only cover directories, and related services, for gTLDs, excluding for instance country code top-level domains (ccTLDs), and the capitalized terms "Whois services" and "Whois data", as used in this memorandum, only comprise services and data relating to gTLDs, as carried out based on the contractual requirements in the agreements between ICANN and registrars and registries.

1.3 Due to the complexity of the issue, we intend to provide a series of memoranda, which will address different aspects of the issue and where the scope and topics

of each such memorandum will be discussed and agreed with ICANN. We understand that ICANN intends to make each memorandum publicly available.

1.4 On 16 October 2017, we published part 1 of our memoranda series (the "**October 2017 Memorandum**"), which focused on the compliance of the Whois services, in their current form, with the GDPR.

1.5 On 15 December 2017, we published part 2 of our memoranda series, in which we addressed certain questions that had been raised by the gTLD community and provided to ICANN following the publication of the October 2017 Memorandum.

1.6 In this part 3 of our memoranda series, we elaborate on how the processing of data within the scope of the Whois services could possibly be changed in order to become compliant with the GDPR.

2. ASSESSMENT

2.1 General approach

2.1.1 In the October 2017 Memorandum, we concluded that consent is not a practically viable legal ground for processing personal data in an efficient way, given the intended use of the Whois services. We also concluded that while the performance of contract legal ground could be used for some processing where the controller has a contract directly with the data subject, it would not be sufficient to motivate the intended use of the Whois services as public directories.

2.1.2 In a letter to ICANN dated 6 December 2017, the Article 29 Working Party communicated a view that is generally consistent with our above assessment. Further, in historic correspondence with ICANN, the Article 29 Working Party has expressed that it acknowledges the use of Whois services for support purposes as a legitimate purpose but that the public access to the Whois data in its current form goes beyond that legitimate purpose. This reasoning is further very much in line with the opinions expressed by CJEU case law and the actions of the EU data protection authorities (each a "**DPA**").

2.1.3 In order to obtain compliance with the GDPR, we will, *inter alia*, discuss a layered access model where different personal data usages within the scope of the Whois services are analyzed to formulate different purposes, requiring access to different types and amounts of data, for different processing activities. We will then aim to assess whether such processing activities can be paired with an applicable legal ground and be minimized so that the processing, and the personal data being processed, is not more extensive than necessary.

2.1.4 Our belief is that several of the purposes for which the Whois data currently is processed (such as for administration actions and law enforcement) could be achieved by using a layered access model where the data necessary for a certain purpose can be accessed only by the parties that actually need it, and that such a layered access model probably could be based on legitimate interest or necessity for performance of contract (or a combination thereof).

2.2 Limitations

2.2.1 For the purpose of this memorandum, we have focused on issues relating to the purposes and legal grounds for processing. We will thus not, except where so required for our assessment, elaborate on all requirements set out in the GDPR that will need to be observed in order to achieve compliance, such as the basic principles for processing, the principles for transfer of personal data to third countries or the information requirements.

2.2.2 As touched upon in the October 2017 Memorandum, data that relates only to a legal person would under the GDPR still constitute personal data if, for instance, the company name includes the name of an identifiable natural person, if the contact address is a natural person's residence or if the e-mail contact address contains the name of a natural person. Opinions differ somewhat as to whether such information should be considered fully equivalent to personal data that relates directly to a natural person, and it can for instance be argued that the threshold for being able to process such "indirect" personal data based on legitimate interest in accordance with Article 6.1(f) GDPR should be lower than what is otherwise the case. For the purpose of this memorandum, we have not made any distinction between different kinds of personal data. Given the vast amount of data being processed within the scope of the Whois services and the large number of parties involved, the primary focus should be to find a solution that treats all types of data the same, as alternatives where different data would need to be processed in different ways would be very challenging for the concerned parties in practice.

2.3 Purposes for Processing

2.3.1 Under the accreditation agreement that ICANN enters into with each of its accredited registrars, the 2013 Registrar Accreditation Agreement (the "**2013 RAA**"), ICANN requires that the registrars collect certain data regarding any registered domain name and the registrants of such domain names and that the collected data is made publicly available through the Whois services. The 2013 RAA further sets out that the registrars shall permit use of the Whois data for "any

lawful purposes except to: (a) allow, enable, or otherwise support the transmission by e-mail, telephone, postal mail, facsimile or other means of mass unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of any Registry Operator or ICANN-Accredited registrar, except as reasonably necessary to register domain names or modify existing registrations".

2.3.2 Despite the fact that abovementioned provision provides very broad boundaries for the processing of Whois data under the 2013 RAA, the purposes for processing of personal data within the scope of the Whois services have historically not been very elaborately described in the communication with the public and the external understanding of the purposes for processing seems to be rather limited. For instance, focus within the gTLD community seems to lie with the use of Whois data for support and technical assistance to registrants, as well as the use of Whois data for law enforcement activities. While these are all purposes that the Whois data is used for, it does not fully explain the use and need of public Whois services. For instance, one of the main objectives of ICANN is to maintain open Whois services and to promote the openness of the internet and it would be incorrect to state that the only purpose of the Whois services is to manage domain name registrations. As stated in the October 2017 Memorandum, ICANN's bylaws sets out that ICANN shall, subject to applicable laws, "use commercially reasonable efforts to enforce its policies relating to registration directory services" and "cause a periodic review to assess the effectiveness of the then current gTLD registry directory service and whether its implementation meets the legitimate needs of law enforcement, promoting consumer trust and safeguarding registrant data".

2.3.3 As a first step, the purposes for processing of personal data within the scope of the Whois services must be determined and formulated in a way that is compliant with the GDPR. Based on the current use of the Whois data, personal data can be said to be processed within the Whois services for the purposes listed below.

(i) The use of Whois data, for instance by registrars and network operators, for invoicing, support and other administration actions in relation to registered domain names.

(ii) The use of Whois data for safeguarding the rights of registrants, for instance by retention of the data in escrow with escrow agents, for recovery in the event of e.g. a distressed registrar or registry or failure by a registrar or registry to fulfill its obligations.

(iii) The use of Whois data by law enforcement agencies to investigate and counter serious crime, terrorism, fraud, consumer deception, intellectual property violations or other violations of law.

(iv) The use of Whois data by intellectual property rights holders to investigate intellectual property rights infringements.

(v) The use of Whois data by the general public to verify the identity of a provider of goods or services on the internet, including for consumer protection purposes.

(vi) The use of Whois data to identify the owner of a domain for business purposes, for instance in relation to a purchase of the domain name or other transactions.

The above list is not intended to be exhaustive but to serve as suggestions for how the Whois services can be viewed from a data processing perspective.

2.3.4 Even if a legitimate purpose and a legal ground can be identified to rely upon for a certain processing activity, the processing must always comply with the general principles for processing laid out in Article 5 GDPR. This means that, among other things, the following must be taken into account:

(i) Only personal data needed for the relevant purpose shall be processed (purpose limitation).

(ii) The processing as such shall be limited to processing that is necessary for the purpose (minimization).

(iii) Only the parties (may it be registrars, registries, ICANN or the general public) that need to process the data for the established purpose shall be able to access it.

2.3.5 Consequently, in light of the general principles, the following questions should be asked when determining the purposes and assessing the potential legal ground for different processing activities:

(i) What Whois data is necessary to fulfill the particular purpose?

(ii) Which parties need to have access to the Whois data for the particular purpose?

(iii) Is there a need for the Whois data to be public for the particular purpose?

2.3.6 In the following, we will discuss to which extent Whois data can be continued to be processed for the purposes identified above also under the GDPR.

2.4 Processing of Whois data for administration actions

2.4.1 In order for a domain name registrant to have a gTLD domain name registered and properly maintained, there is a need for ICANN, registrars and registries to process personal data for the purpose of performing different administration actions, such as invoicing, support and technical assistance. The exact needs for different parties will vary based on the relation with the registrant (where for instance only the contracting party registrar might have a need to process personal data for invoicing but where other parties might have a need to process personal data for technical reasons or providing technical assistance).

2.4.2 Registrars that enter into contracts directly with the registrants should be able to process personal data based on that the processing is necessary to perform such contracts, i.e. to comply with their contractual obligations, in accordance with Article 6.1(b) GDPR.

2.4.3 Where the data controller is not a party to the contract with the registrant, which is the case for ICANN and the registries, performance of a contract in accordance with Article 6.1(b) GDPR cannot be used as legal ground for processing for administration actions. However, it should be possible to base such processing on legitimate interest as legal ground in accordance with Article 6.1(f) GDPR as long as the processing is limited to what is necessary, given the purpose.

2.4.4 It should be fairly uncontroversial to state that there exists a legitimate interest for certain parties to process personal data for administration actions, as outlined above. Even in the cases where the controller is not the contracting party, this processing is necessary in order for the registrant to register and maintain a domain name. Similarly, the possible interests of the registrant for not having personal data processed, as long as the processing is adequately limited, should be very limited or even non-existent.

2.4.5 While, as stated above, processing of personal data for administration actions by all accounts constitute a legitimate interest and while there should be no real reasons against the processing in light of the interests or fundamental rights or freedoms of the registrant, the processing must still be in compliance with the general principles for processing, as described in sections 2.3.4 and 2.3.5 above. In light of these principles, our assessment is that the data to be processed for administration actions likely can be rather extensive (where for instance the registrars would need to process contact data and registries would need to

process more technical data, such as IP-addresses) but that the access to the data must be limited to the parties that actually needs it in light of the relevant purpose. As a consequence, the purposes described in this section 2.4 cannot be used to motivate the publication of the Whois data in public directories.

2.5 Processing of Whois data for recovery purposes in case of distress etc.

2.5.1 In order to maintain a reliable system for the management of gTLD domain names, it is necessary to be able to recover Whois data in the event that a registrar or a registry is unable to perform its obligations under its agreement with ICANN and, ultimately towards the registrants. For this purpose, registrars are required under the 2013 RAA and registries are required under the registry agreement entered into with ICANN to deposit Whois data with an escrow agent designated or approved by ICANN (a Registrar Data Escrow Agent) for release to ICANN or a party designated by ICANN in case of termination of the 2013 RAA or the registry agreement, as applicable, including but not limited to termination due to the registrar's or registry's bankruptcy or breach of contract.

2.5.2 In line with the arguments for processing of Whois data for administration actions laid out in section 2.4 above, it should be possible to base processing for disaster recovery purposes on legitimate interest as legal ground in accordance with Article 6.1(f) GDPR as long as the processing is limited to what is necessary, given the purpose.

2.5.3 As in the case with processing of Whois data for administration actions, processing for disaster recovery purposes cannot be used to motivate publication of the Whois data in public directories, as it is possible to fulfill these purposes without making the Whois data publicly available.

2.6 Processing of Whois data for law enforcement purposes

2.6.1 The current Whois services are used by law enforcement agencies to, *inter alia*, investigate and counter serious crime, terrorism, fraud, consumer deception, intellectual property violations or other violations of law.

2.6.2 Processing of Whois data by law enforcement agencies for such law enforcement purposes should constitute a legitimate interest that motivates processing of personal data in accordance with Article 6.1(f) GDPR. As in the case with processing of Whois data for administrative actions, processing for law enforcement purposes can however not be used to motivate publication of the Whois data in public directories, as it should be possible to fulfill the needs of the law enforcement agencies without making the Whois data public.

2.6.3 As will be discussed further in section 2.7, a layered access model does not automatically qualify as legal ground to disclose personal data to a pre-determined group of parties, including law enforcement agencies, even where a legitimate interest has been identified and determined on a general level. For instance, Article 6.1(f) GDPR can most likely not be used to provide all law enforcement agencies unfiltered access to all Whois data but such access would likely have to be assessed in light of Article 6.1(f) GDPR, with the appropriate balancing of interests, in each case. As an example, the Court of Justice of the EU (the "**CJEU**") ruled in Case C-203/15 (*Tele2 Sverige*) and Case C-698/15 (*Watson*) that although the EU Privacy and Electronic Communications Directive 2002/58 allowed for law enforcement agencies to access traffic data (including personal data) retained by telecommunication service providers for the purpose of fighting serious crimes, such a right could not be extended to a right to access all such retained data without sufficient links to the relevant purpose.

2.6.4 In the abovementioned CJEU cases, the CJEU also stated that access to retained data by competent law enforcement agencies as a general rule must, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those law enforcement agencies submitted, *inter alia*, within the framework of procedures for the prevention, detection or prosecution of crime. Although the referenced CJEU cases, in part, concerned different kinds of data for different purposes than what is the case in relation to the Whois services, the CJEU clearly established that disclosure to law enforcement agencies for crime fighting purposes should primarily be tried and decided by competent courts.

2.6.5 In light of the above, the practical details and mechanics for enabling processing for law enforcement purposes need to be assessed specifically and will not be covered by this memorandum. For instance, it needs to be analyzed how requests by law enforcement agencies to access Whois data should be handled in practice, for instance if such requests can be processed by the registrars or whether they need to be made subject to approval from relevant courts, and if any distinction should be made between EU and non-EU law enforcement agencies when assessing whether to provide access to the data.

2.7 Processing of Whois data by rights holders and others for investigation of fraud, consumer deception, IP infringements etc.

2.7.1 While law enforcement is often emphasized as a legitimate interest for processing Whois data, other parties may also have a legitimate interest to access Whois

data for similar purposes. In this regard, it can be argued that there exists a legitimate interest for entities and private individuals to be able to identify a domain name holder for *inter alia* the following purposes:

(i) In the event of potential fraudulent actions. For instance, it has become common that fraudulent invoices are sent to companies and private individuals. One key element when trying to verify whether these invoices, and similar correspondence, are legitimate is to check the holder of the domain name held by the sender.

(ii) In the event of potential trademark infringements. Holders of registered and unregistered trademarks and similar rights have a legitimate need to assess whether a registered domain name infringes their rights. In order to make such an assessment, it is necessary to verify the identity of the domain name holder so that the business for which the domain name is used can be identified an assessed in relation to the holder's trademarks.

(iii) In the event of infringement of copyrights, patents or other intellectual property rights. Holders of copyrights, patents or other intellectual property rights have a legitimate need to identify the party behind a potential infringement, relating to for instance unlawful sharing of music, film, software or photos or unlawful use of patented processes.

(iv) In relation to the purchase of goods and services. Also in cases where there is no suspicion of fraud, there exists a legitimate need for a purchaser of goods or services, especially when such purchaser is a consumer, to be able to verify the identity of the provider of such goods or services. For instance, if medical services are offered on a website, potential customers need to be able to verify that the service provider has the necessary qualifications and licenses etc.

(v) For maintaining a secondary market for purchase of domain names. It is undeniable that finding the right domain name is essential when starting a business or changing the brand of an existing business. As a logical consequence hereof, there exists a need to be able to approach the owner of a registered domain name for transaction purpose as well as a related need to verify that an alleged owner of a domain name in fact is the owner.

2.7.2 All of the purposes listed in section 2.7.1(i) - (v) above would in our opinion qualify as legitimate interests for the concerned parties. However, in order to constitute legal ground for processing in accordance with Article 6.1(f) GDPR, these interests

must be weighed against, and override, the interests or fundamental rights and freedoms of the data subject, i.e. the registrants.

2.7.3 When balancing the interests of the controller (or a third party) and the data subject in accordance with Article 6.1(f) GDPR, it should be taken into account how sensitive and invasive the data processing is for the data subject. By limiting the personal data being processed, the sensitivity and invasiveness of the processing can for instance be decreased. In relation to the purposes listed in section 2.7.1(i) - (v) above, it should be assessed which data that really needs to be processed in order to fulfill the purposes. For the purposes listed above, the legitimate interest consists of being able to identify and contact the registrant and it should be sufficient to access the name and address of the registrant (which would mean removing e-mail addresses, which are publicized today) to fulfill this need (this is also the information that is made public in other registers of similar kind, such as trademark registers).

2.7.4 In the assessment of how the personal data to be processed can be minimized in light of the relevant purpose, our assessment is that access to the e-mail addresses of registrants which are natural persons is not necessary for the purposes listed in 2.7.1(i) - (v) above and that such e-mail addresses therefore should not be made publicly available through the Whois services.

2.7.5 In relation to the balancing of interests in accordance with Article 6.1(f) GDPR, it can be discussed whether the Whois data (i.e. the identity and address of the registrant) needs to be publicly available. As outlined in the October 2017 Memorandum, the opinion of both the Article 29 Working Party and the DPAs appears to be that legitimate interest in accordance with Article 6.1(f) GDPR cannot be used to legitimize making personal data publicly available through the Whois services. In line with this stance, different parties within the gTLD community has discussed layered access levels for some of the purposes above (for instance with regard to intellectual property rights holders investigating potential infringements), where the Whois data would be held by the registrars and not be publicly accessible, however that the public (such as rights holders) may request access to additional information for certain purposes. It has also been suggested that some types of parties, such as intellectual property lawyers, should be able to automatically qualify to access such additional information.

2.7.6 We see several practical issues with such a layered access model for the above purposes. To start with, having layered access levels does not automatically qualify as legal ground. If a registrar receives a request from the public to disclose additional data, the registrar must then, in each individual case, assess whether

legal ground to disclose such data exists. In practice, the registrar would have to perform an assessment of whether sufficient legitimate interest exists in accordance with Article 6.1(f) GDPR and whether or not the interests or fundamental rights and freedoms of the registrant override such interest. This would require each registrar to maintain both the competence to make such an assessment and the internal organizational and technical routines and measures to handle such requests on a large scale. This is in our opinion not a realistic requirement to place on registrars.

2.7.7 Having "automatically qualified parties" would face similar challenges. Having such automatically qualified parties requires that it must be possible to, on a general basis, determine that a certain type of party always is qualified to access certain data based on Article 6.1(f) GDPR (or any other legal ground set out in Article 6.1 GDPR). As discussed in sections in sections 2.4 and 2.5 above, our opinion is that this kind of solution should be possible for administration purposes and disaster recovery purposes, as it should be possible to state that all parties of a certain category within the gTLD community (and accredited by ICANN) has a sufficient legitimate interest to process Whois data for certain actions. This type of generalized assessment is however, in our opinion, very difficult to apply in order to automatically qualify, for instance, intellectual property lawyers or similar categories to access data that is not permitted to publish publicly. Even if a lawyer in its own capacity could be accredited to access additional data, this does not mean that the qualifications for processing pursuant to Article 6.1(f) GDPR are met for the lawyer's client. Given that the lawyer's primary objective always will be, and must be, to protect the interest of the client, it will not be possible to disclose Whois data to a lawyer without having secured that the data can also be disclosed to the lawyer's client.

2.7.8 Holders of intellectual property rights have an opportunity under the EU Enforcement of Intellectual Property Rights Directive 2004/48/EC ("**IPRED**") to request competent judicial authorities to order an infringing party to provide information on the origin and distribution networks used to commit the infringement. Such an order may also be given to a party that is providing commercial scale services used in the infringing activities, including for instance telecommunication providers. Depending on the implementation of IPRED through national legislation in the different EU member states, such judicial orders could possibly also be given to a registrar or registry to disclose the identity of a registrant.

2.7.9 Even if IPRED could be used to investigate potential infringements of trademarks, copyrights, patents and other intellectual property rights, there is still a legitimate

need for intellectual property rights holders to be able to use Whois services to investigate and assess potential infringements before requesting an order from a judicial authority. Further, it would risk putting courts and other authorities under significant pressure if there was no easily accessible way to access relevant information other than requesting a judicial order.

2.7.10 In light of the above reasoning, our opinion is that it will not be practically feasible to fulfill the purposes listed under this section 2.7 through a layered access model, as such a model would require the registrars to perform an assessment of interests in accordance with Article 6.1(f) GDPR on an individual case-by-case basis each time a request for access is made. This would put a significant organizational and administrative pressure on the registrars and also require them to obtain and maintain the competence required to make such assessments in order to deliver the requested data in a reasonably timely manner. In our opinion, public access to (limited) Whois data would therefore be of preference and necessary to fulfill the above purposes in a practical and efficient way. In section 2.8 below, we will discuss if such public access could be possible in light of the GDPR.

2.8 Outlook and comparison with other services

2.8.1 General

2.8.1.1 As outlined above, our assessment is that there exists a legitimate interest for making Whois data publicly available, at least in limited parts, and that it will come down to whether such interest are overridden by the interests or fundamental rights and freedoms of the data subject.

2.8.1.2 When assessing whether the interests or fundamental rights and freedoms of the registrants are threatened by the publication of the Whois data, the extent of both the data being published and of the publication must be taken into account. Within the scope of the purposes listed in section 2.7 above, a limited part of the Whois data (i.e. the identity and address of the registrant) would be made publicly available on the internet through the Whois services. In order to assess whether such publication could at all be possible in light of the GDPR, it is relevant to see how these categories of personal data is being processed and made available in other registers of similar kind.

2.8.1.3 In most EU member states, there are a number of different public registers that contain publicly accessible personal data, such as company registers, real property registers, trademark registers, patent registers and design right registers. In the following, we will take a closer look at some such registers, in particular the register for EU trademarks ("**EUTM Register**"), which is kept and managed by the European Union Intellectual Property Office ("**EUIPO**").

2.8.2 Trademark registers

2.8.2.1 The EUTM Register is relevant as a comparison since trademarks and domain names have many similarities and in many ways are treated as similar rights and used for the same purposes. For instance, when choosing a brand, it is as important to secure the relevant domain names as to register the relevant trademarks.

2.8.2.2 The EU Trademark Regulation 2017/1001 (the "**EUTMR**") states that EUIPO shall keep a register of all EU trademark applications and registrations. Article 111 EUTMR explicitly requires that such register shall, among other things, contain the name and address of any applicant and that the register shall be updated with any changes in the name or address. It is further explicitly stated that the EUIPO shall collect, store and make public the required registration data, including the aforementioned personal data, and keep it easily accessible for public inspection.

2.8.2.3 It is particularly noted that Article 111.9 EUTMR states that all the data, including personal data, to be recorded in the trademark register, shall be considered to be of public interest and may be accessed by any third party. Also, any entries in the register shall be kept for an indefinite period of time.

2.8.2.4 As recapitulated in Recital (1) GDPR, Article 8.1 of the Charter of Fundamental Rights of the European Union (the "**Charter**") states that "everyone has the right to the protection of personal data concerning him or her". While this right is not absolute, any limitations to it must take into account the principle of proportionality, as set out in Article 5 of the Treaty on the European Union. As a consequence, limitations to the rights set out in the Charter, including any limitations stipulated under EU regulations, such as an obligation to record personal data in the EU trademark register, must comply with the principle of proportionality and be limited to what is necessary. The foregoing is for instance illustrated in Case C-293/12 (*Digital Rights Ireland*) and C-594/12 (*Seitlinger and others*), where the CJEU ruled that the EU legislator, when adopting the EU Data Retention Directive 2006/24 exceeded its limits imposed by compliance with the principle of proportionality in light of, *inter alia*, Article 8 of the Charter.

2.8.2.5 In addition to the legal grounds for processing discussed in this memorandum, Article 6.1(e) GDPR sets out that processing of personal data shall be considered lawful if and to the extent that it is necessary for the performance of a task carried out in the public interest. In this context, "public interest" is basically limited to processing activities that are explicitly allowed under law. However, when allowing certain processing to be codified into law, the legislator must consider the legal grounds for processing, including the balancing of the interest of processing personal data against the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

2.8.2.6 In relation to the EUTM Register, as clearly evidenced by and set out in Article 111 EUTMR, the EU has considered it a public interest to keep a public record of the owners of any EU trademarks and has, as must be understood, as a part of that consideration, implicitly stated that such interest overrides the interests or fundamental rights and freedoms of the trademark registrants. At the same time, the opinion of the Article 29 Working Party and the DPAs appears to be that the legitimate interests to keep a register of equivalent information for gTLD domain names is not strong enough to override the interests or fundamental rights or freedoms of the domain name registrants. In our assessment, we have had difficulties seeing the difference between a trademark register and a domain name register from a public interest and integrity protection perspective and it can be argued whether or not such a distinction is in fact proportionate.

2.8.3 ccTLD registers

2.8.3.1 EU Regulation 733/2002 regulates the implementation of the .eu ccTLD. The regulation prescribes the administration and management of "public query services" (i.e. Whois services) for .eu domain names and states, in Recital (12), that "whois type databases" are "an essential tool in boosting user confidence" and that such databases should be in conformity with EU law on data protection and privacy.

2.8.3.2 Further, EU Commission Regulation 874/2004 states that the purpose of the whois database for .eu domain names shall be to "provide reasonably up to date information about the technical and administrative points of contact administering the domain names under the .eu TLD" and that the database shall contain information about the holder of a domain name that is relevant and not exessive in relation to the purpose of the database. In as far as the information is not strictly necessary in relation to the purpose of the database and if the holder of the domain name is a natural person, the information that is to be made publicly available shall be subject to unambiguous consent of the domain name holder.

2.8.3.3 The above ties in well with the discussion above in this memorandum, as it essentially states that personal data can be processed in a whois database to the extent such processing is necessary for the purpose of the database, and that such personal data should be minimized to the extent possible. As previously discussed, the purpose of the gTLD Whois services goes beyond the purpose explicitly stated in EU Commission Regulation 874/2004 referenced above, where the latter purpose is limited to providing technical and administrative points of contact. In this context, it should however again be noted that EU Regulation 733/2002 states that access to public whois type databases is an essential tool in boosting user confidence, which also stretches beyond the providing of technical and administrative points of contact.

2.8.3.4 In Finland, the Finnish Information Society Code states that the body managing the domain name register for the .fi ccTLD may disclose information from the domain name register, and that information regarding registrants that are natural persons shall be limited to the domain name and the name of the registrant. The Finnish legislator here appears to have made the assessment that the name of a registrant that is a natural person is necessary for the purpose of the whois database for .fi domains.

2.8.4 Company registers

2.8.4.1 Company registers throughout the EU member states contain certain personal data, such as the identity of board members. In Case C-138/11 (*Compass-Datenbank*), the CJEU held that the activity of a public authority consisting in the storing, in a database, of data which undertakings are obliged to report on the basis of statutory obligations, permitting interested persons to search for that data and providing them with print-outs thereof, falls within the exercise of public powers and that such an activity also constitutes a task carried out in the public interest.

2.8.4.2 In Case C-398/15 (*Manni*), the CJEU considered the right of natural persons to have their personal data removed from company registers. In the referenced case, the director of an Italian company wanted his personal data removed from the company register because, in his view, properties in a tourist complex built by his company were not sold because it was clear from the company register that he had been the representative of another company that went bankrupt in 1992 and was wound up in 2005.

2.8.4.3 The CJEU noted that the EU member states cannot guarantee that natural persons whose data are included in a company register have the right to, after a certain period of time from the dissolution of the company, have the personal data concerning them erased. The CJEU considered that this interference with the fundamental rights of the persons concerned (including the right to protection of personal data guaranteed by the Charter) is not disproportionate in so far as (i) only a limited number of personal data items are entered in the company register and (ii) it is justified that natural persons who choose to participate in trade through such a joint stock company or limited liability company, whose only safeguards for third parties are the assets of that company, should be required to disclose data relating to their identity and functions within that company.

2.8.4.4 Nevertheless, the CJEU did not exclude the possibility that, in specific situations, overriding and legitimate reasons relating to the specific case of the person concerned may justify, exceptionally, that access to personal data concerning that person should be limited, upon expiry of a sufficiently long period after the dissolution of the company in question, to third parties who can demonstrate a specific interest in consulting that data. Such limitation of access to personal data must be based on a case-by-case assessment.

2.8.5 Conclusion

In light of the above, we think that the arguments behind the EUTM Register according to the EUTMR, as well as the arguments referred to above relating to ccTLDs and company registers, are worth considering in relation to the Whois services in light of the GDPR and that this is something that deserves to be properly assessed by the DPAs, as is described in section 3.4 below.

3. CONCLUSIONS AND POSSIBLE WAYS FORWARD

3.1 General

3.1.1 As discussed above, there are certainly arguments for that a continuance of public Whois services in some form could be possible also under the GDPR. However,

due to the uncertainty of how the GDPR will be interpreted and applied by the DPAs, in combination with DPAs' apparent view on the Whois services as non-compliant with the GDPR as currently provided, it would in our opinion not be advisable to continue to provide publicly available Whois services in an unchanged manner under the current circumstances and conditions until further clarity has been obtained on how the GDPR will be applied and enforced by the DPAs.

3.1.2 Our advice would instead be to try to identify and adapt a model where certain limited purposes of the Whois services can continue to be fulfilled on 25 May 2018 when the GDPR enters into effect, as is described in section 3.2 below. However, we would also recommend ICANN to consider an informal dialogue with the Article 29 Working Party, as further described in section 3.3 below, and initiate formal consultations with DPAs, as further described in section 3.4 below, in order to find a solution where Whois services can continue to be provided in a form available to the general public in the future.

3.1.3 The actions summarized in sections 3.2 - 3.4 below should be seen as complements to each other rather than alternative suggestions and should all be useful tools for establishing a workable solution for processing Whois data.

3.2 Implementing a layered access model

3.2.1 Given the limited time remaining until the GDPR enters into effect, we believe that the best chance of continuing to provide the Whois services and still be compliant with the GDPR will be to implement an interim solution based on an layered access model that would ensure continued processing of Whois data for some limited purposes. Some basic thoughts on how to construct such purposes and such a model are laid out in sections 2.4 - 2.6 above. The exact purposes and mechanics for such a model however need to be analyzed in depth.

3.2.2 Applying a layered access model as described in sections 2.4 - 2.5 above could secure the use of Whois data for administration and disaster recovery purposes, which would allow the most basic functions of the gTLD system to continue to function, and adding an additional layer as described in section 2.6 (however noting the challenges identified in section 2.6) could provide for the continued use of Whois data for law enforcement purposes (in addition to any law enforcement already provided for under national EU member state law), and we see this as a possible and workable temporary solution, while further investigating a workable long-term model that would also enable the purposes described in section 2.7 above.

3.3 Informal dialogue with the Article 29 Working Party

3.3.1 In parallel with implementing an interim layered access model for use as from 25 May 2018, we would recommend ICANN to continue to explore the possibility of having publicly available Whois services in the future. In order to seek clarity over such possibilities, there are possibilities to engage both on an informal basis with the Article 29 Working Party, and on a formal basis with the DPAs through data protection impact assessments (each such assessment a "**DPIA**"), as further described in section 3.4 below.

3.3.2 The Article 29 Working Party, which will be replaced by a new European Data Protection Board when the GDPR enters into force, has opened for a dialogue with ICANN. Engaging more into such a dialogue than what has historically been the case could give ICANN a good opportunity to express and clarify its view on data processing in relation to the Whois services going forward both from a short and long term perspective.

3.3.3 Although this approach has its advantages, it also has some limitations. For instance, the Article 29 Working Party's has no obligation to respond to queries of this kind or to provide any opinions to any others parties than any of the DPAs or the EU commission other than on an *ex officio* basis. It shall also be noted, that any communications, opinions, guidelines, etc., expressed by the Article 29 Working Party are not legally binding in relation to controllers and processors and cannot be appealed. As a consequence, there is no guarantee that ICANN can rely on its correspondence with the Article 29 Working Party, as it is up to the DPAs to apply and enforce the GDPR. Although the DPAs are normally aligned with the view of the Article 29 Working Party, this is not automatically the case. Further, as any advice from the Article 29 Working Party, by its nature, tend to be general and on a principal level, any principles agreed or implied need to be adapted into actual processing, which will ultimately be tried by the DPAs.

3.3.4 Further, the Article 29 Working Party has since its initial correspondence with ICANN in 2003 suggested a layered access model. As discussed in this memorandum, it should be possible to establish layered access models, for instance in line with the principles discussed in sections 2.4 - 2.6 above, that enable processing of personal data in compliance with the GDPR for some limited purposes. Based on previous communication, the view of the Article 29 Working Party appears to be that such limited processing is sufficient. However, as described above, in order to fulfill the purposes set out in ICANN's bylaws and the purposes discussed in section 2.7, there is a need for public Whois services as

well, and it is uncertain whether such a change in principle can be achieved solely through informal dialogue.

3.3.5 In summary, the non-binding and non-appealable nature of any communications with the Article 29 Working Party adds an element of uncertainty that in our opinion will make it difficult to rely solely on such communications. Thus, although a dialogue with the Article 29 Working Party is advisable and will surely be a very helpful tool, further actions are likely necessary in order to establish that publicly available Whois services could be compliant with the GDPR.

3.3.6 In light of the above, we would as a first step recommend ICANN to explore the possibility to engage in discussions with the Article 29 Working Party Group, and that such discussions are followed by the filing of a formal DPIA, as further described in section 3.4 below.

3.4 Data protection impact assessment

3.4.1 As described in the October 2017 Memorandum, the GDPR encourages, and requires in cases where a processing activity is "likely to result in a high risk to the rights and freedoms of natural persons", controllers to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a DPIA).

3.4.2 Where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller shall consult the applicable DPA.

3.4.3 Where the DPA is of the opinion that the intended processing described in the DPIA would infringe the GDPR, the DPA shall, within a period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller. That period may be extended by six weeks, taking into account the complexity of the intended processing and both the said periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3.4.4 As described in section 2.8 above, we are of the opinion that there are legitimate arguments for that public Whois services could potentially continue to exist in some form also under the GDPR, but that this view is not consistent with the view that has been expressed by the Article 29 Working Party and the DPAs, based on current provision of unlimited and non-layered access to Whois data without clear descriptions of the purposes for processing. In order to attempt to solve this issue and establish a common view on the public Whois services, where the alternative

would be to close down the public availability, we would propose that ICANN, in addition to engaging in informal discussions with the Article 29 Working Part, prepares and submits a DPIA to the DPA in an EU member state where ICANN has an established presence. Such a DPIA should include the measures for compliance taken, for instance the implementation of a layered access model and clearly described purposes for processing.

3.4.5 Where a DPIA is required for a processing activity for which there are joint controllers, a DPIA would have to be carried out by all joint controllers. In the October 2017 Memorandum, we recommended to take ta general view that ICANN, the registrars and the registries are all considered to be joint controllers. In light thereof, it needs to be further assessed how and by whom the DPIA formally should be prepared and filed.

3.4.6 Filing a DPIA would at the very least create a discussion with the DPA regarding the public availability of the Whois services and provide the DPA with the opportunity to communicate its view on the matter.

_____