

Differentiation between Legal and Natural Persons in Domain Name Registration Data Directory Services (RDDS)

Prepared per Recommendation 17.2 of the Final Report of the Expedited Policy Development Process Team on the Temporary Specification for gTLD Registration Data (Phase 1)

ICANN Org Policy Research and Data Services: July 2020

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
RESEARCH DESIGN AND METHODOLOGY	6
RESEARCH QUESTIONS.....	9
QUESTIONNAIRE	10
DIFFERENTIATION AND THE GDPR	12
CURRENT POLICY AND RECOMMENDATIONS.....	15
DIFFERENTIATION: PROBLEMS AND PROSPECTS	17
RISKS AND COSTS: THE BURDEN OF DIFFERENTIATION BY PARTY	19
<i>Contracted Parties</i>	19
<i>Data Subjects</i>	23
<i>RDDS End-Users</i>	24
EASING THE BURDEN OF DIFFERENTIATION: METHODS TO MITIGATE RISKS AND COSTS.....	28
<i>Contracted Parties</i>	28
<i>Data Subjects</i>	34
<i>RDDS End-Users</i>	34
<i>Collective Mitigation Efforts</i>	34
BENEFITS: RDDS AS A COLLECTIVE GOOD.....	36
<i>Contracted Parties</i>	39
<i>Data Subjects</i>	40
<i>RDDS End-Users</i>	42
FEASIBILITY	43
<i>Differentiation in Practice</i>	45
DIFFERENTIATION SCENARIO MODEL	60
IMPORTANT NOTES AND CAVEATS	60
MODEL KEY.....	62
PROBLEM SYNOPSIS	63
<i>Variables and Measurement</i>	63

FEASIBILITY ASSESSMENT HEAT MAP KEY	67
SCENARIO 0: NO DIFFERENTIATION	69
SCENARIO 0: “NO DIFFERENTIATION” PROCESS MAP.....	70
SCENARIO 0: “NO DIFFERENTIATION” FEASIBILITY ASSESSMENT HEAT MAP	71
SCENARIO 0: “NO DIFFERENTIATION” FEASIBILITY VALUE BY PARTY	72
SCENARIO 1: REGISTRANT SELF-IDENTIFICATION	73
SCENARIO 1: REGISTRANT SELF-IDENTIFICATION PROBLEM MAP.....	74
SCENARIO 1 (REGISTRANT SELF-IDENTIFICATION): FEASIBILITY ASSESSMENT HEAT MAP	75
SCENARIO 1 (REGISTRANT SELF-IDENTIFICATION): FEASIBILITY VALUE BY PARTY.....	76
SCENARIO 2: DIFFERENTIATION BY CONTRACTED PARTY	77
SCENARIO 2: DIFFERENTIATION BY CONTRACTED PARTY PROBLEM MAP.....	78
SCENARIO 2 (DIFFERENTIATION BY CONTRACTED PARTY): FEASIBILITY ASSESSMENT HEAT MAP	79
SCENARIO 2 (DIFFERENTIATION BY CONTRACTED PARTY): FEASIBILITY VALUE BY PARTY	80
CONCLUSION	81
REFERENCES	83

Executive Summary

Recommendation 17.2 from the Expedited Policy Development Process Team on the Temporary Specification for gTLD Registration Data (EPDP) recommend that ICANN org carry out a study on the costs and benefits of differentiating between legal and natural persons in domain name registration data directory services (RDDS).¹ Their Recommendation is as follows:²

The EPDP Team recommends that as soon as possible ICANN Org undertake a study, for which the terms of reference are developed in consultation with the community, that considers:

1. The feasibility and costs including both implementation and potential liability costs of differentiating between legal and natural persons;
2. Examples of industries or other organizations that have successfully differentiated between legal and natural persons;
3. Privacy risks to registered name holders of differentiating between legal and natural persons; and
4. Other potential risks (if any) to registrars and registries of not differentiating

As requested in Recommendation 17.2, ICANN org consulted with the EPDP Team to develop the terms of reference for this report. At the November 2019 public meeting in Montreal (ICANN66), the parties discussed a study that would examine the effects of differentiation between legal and natural persons in RDDS (hereafter “differentiation/differentiating”) on various stakeholders within the RDDS ecosystem, namely domain name registries, registrars, and registrants, as well as parties such as law enforcement, dispute resolution service providers, academia, and others who utilize domain

¹ “Registration Data” means data collected from a natural and legal person in connection with a domain name registration. “Registration Data Directory Services” refers to the collective of WHOIS, Web-based WHOIS, and RDAP services. See: ICANN.org (25 May 2018), *Temporary Specification for gTLD Registration Data*, <https://www.icann.org/resources/pages/gtld-registration-data-specs-en>.

² ICANN GNSO (20 February 2019), *Final Report on the Temporary Specification for gTLD Registration Data Expedited Policy Development Process*, <https://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf>, p. 17.

name registration data for a variety of legitimate legal purposes.³ For the purposes of this study, these stakeholders have been categorized into three groups: **Contracted Parties** (ICANN-accredited domain name registries and registrars), legal and natural person **registrants** (“**data subjects**”), and **RDDS end-users**. They are defined as follows:

Contracted parties: Registrar and registry entities who have contracts with ICANN to provide registration services, support domain name registrants, maintain registration data, and operate registration data directory services.

RDS data subjects: Legal and natural person registrants who interact with and provide data to a registration service provider in the course of an initial registration, domain name transfer, or other transactions during the life of a domain name registration. Generally, a data subject is any person whose personal data is being collected, held or processed.

RDS data end-users: Parties such as law enforcement, dispute resolution service providers, and others who obtain, access, and make use of registration data for a variety of purposes.

The report serves as an informational input to the EPDP Phase 2 Team’s deliberations. It does not provide recommendations or normative assessments of differentiation as a policy issue. It does provide:

1. An introduction to differentiation from a legal and policy perspective, in particular as it relates to processing domain name registration data under the European Union’s General Data Protection Regulation (GDPR)
2. A presentation of differentiation’s problems and prospects as they relate to Contracted Parties, registrants, and RDDS end-users, framed in terms of **cost**, **risk**, **cost-risk mitigation**, and **benefit** for each party and to the RDDS ecosystem as a whole.
3. Examples of differentiation in- and outside the DNS ecosystem.

³ For a transcript of the discussion, see: ICANN.org (2 November 2019), “GNSO - EPDP Phase 2 Meeting (1 of 4)”, <https://66.schedule.icann.org/meetings/1116817>.

4. Analysis based on the results of the questionnaire on differentiation sent to the EPDP Team and circulated amongst the ICANN community.
5. A model derived from the research carried out in points one through four to help the EPDP Team assess: 1) how various technical and legal aspects of differentiation may interact under different policy scenarios; 2) the extent to which differentiation may impose risks and costs on Contracted Parties, registrants, and RDDS end-users; and 3) the potential impact of measures to mitigate the risks and costs of differentiation and the potential benefits it may provide to these parties. The model provides a framework for the EPDP Team to characterize the overall feasibility of implementing a differentiation method.

The report finds that **differentiation would, in effect, redistribute the risks and costs** associated with processing RDDS data. **RDDS end-users** noted a number of **risks** and **costs** from having access to **fewer RDDS data** as a result of the data redaction and protection requirements contained within the GDPR and *Interim Policy* (e.g. decreased cybercrime and/or intellectual property enforcement capabilities). However, the model presented herein illustrates how this redistribution of risks and costs may play out were differentiation a policy requirement. In such a scenario, **Contracted Parties** would bear many of the **costs** and **risks** associated with differentiation, such as the **cost** of devising and implementing an **accurate and reliable method to differentiate**, as well as the **risk of legal liability** should such a method fail to accurately differentiate and personal data are processed in violation of the GDPR as a result. Further, many natural person registrants benefit from the data protections enshrined in the GDPR, and differentiation may result in some small proportion of natural person registrant RDDS data being published as a result of error or negligence. But the **benefits** of differentiation, as well as the impact of measures to **mitigate the risks and costs** of differentiation, may outweigh these risks and costs under a scenario in which differentiation is a policy requirement. It remains for the EPDP Team to determine the relative balance of these factors as they deliberate on the topic.

Research Design and Methodology

The exploratory nature of the research questions posed in Recommendation 17.2 do not lend themselves to deductive (theory-based) research; rather, they call for an inductive (theory-building) approach to help identify general principles regarding differentiation and its potential impact on Contracted Parties, registrants, end-users, and the RDDS ecosystem as a whole. To the extent established theory can be drawn upon, this report looks at differentiation as a *collective action problem*: a situation in which the members of an interest group would benefit from cooperation to achieve an outcome, but do not as a result of particular disincentives facing individual members of the group.⁴

In *The Logic of Collective Action*, Olson argued that large groups face higher costs in organizing to provide public goods for their constituents than smaller groups. This is based on the rationale that as groups become larger, interests become more diverse, and each individual actor has more incentives to “free ride” on the work of others. The collective goods achieved through collective action are enjoyed by all, but pursued by few. Without strong selective incentives—i.e. benefits provided to group members for participation—few group members will actively participate in pursuing them. He states:

First, the larger the group, the smaller the fraction of total group benefit any person acting in the group interest receives, and the less adequate reward for any group- oriented action...Second...the larger the group...the less the likelihood that any small subset of the group, much less any single individual, will gain enough from getting the collective good to bear the burden of providing even a small amount of it...Third, the larger the number of members in the group the greater the organization costs, and thus the higher the hurdle that must be jumped before any of the collective good at all can be obtained...very large groups normally will not, in the absence of coercion or separate, outside incentives, provide themselves with even minimal amounts of a collective good.⁵

⁴ Olson, Mancur (1971), *The Logic of Collective Action: Public Goods and the Theory of Groups*, Cambridge: Harvard University Press

⁵ *Ibid.*, p. 48.

Olson argued that the primary objective of collective action for groups of any size is the provision of collective (or “public”) goods, which he defined as “any good such that, if any person...in a group...consumes it, it cannot feasibly be withheld from others in the group”.⁶ He continues: “*the achievement of any common goal or the satisfaction of any common interest means that a public or collective good has been provided for that group* [italics in original]”.⁷ Olson’s theory of collective action begins with the premise that group behavior cannot be explained simply as the amalgamated sum of the rational, self-interested preferences of a group’s constituents. A common interest in an outcome does not mean a group will efficiently organize to achieve that outcome. *Ceteris paribus*, smaller groups in which members share specific interests will organize more efficiently to advance those interests than larger groups, who face more significant costs in terms of reaching consensus among a larger amount of members.

However, as with any collective good, some parties bear the burden of providing it, while the benefits are enjoyed by parties who do not. For example, emissions standards for automobiles impose a cost car manufacturing companies in an effort to provide the collective good of cleaner air. These standards also carry risks should a manufacturer not comply with them, as evidenced by the case of Volkswagen, who was caught falsifying the results of their in-house emissions tests in 2017.⁸ A collective action problem arises when the benefits of a collective good are recognized, but those smaller parties who would bear the burden of providing it are unable or unwilling to do so.

In Olson’s original formulation, group size was a key determinant in whether individual, self-interested behavior would translate into effective group action and the provision of public goods for the group. The larger the group, the more fractional the potential individual benefit from collective action. The larger the group, the more likely it is to have members who “free ride” on the work of others. Anyone who has worked on a group project knows that certain members may not contribute as much as others, yet enjoy the benefits of the outcome produced (the ire of hard-working group members notwithstanding). Olson calls groups in which no individual has an incentive to act because their action, or inaction, does not affect other group members, a “latent” group. Only through coercion or the provision of “selective incentives”—benefits that go only to group members—will members of

⁶ *Ibid.*, p. 14.

⁷ *Ibid.*, p. 15.

⁸ Leggett, Theo (12 January 2017), “VW papers shed light on emissions scandal”, *bbc.com*, <https://www.bbc.com/news/business-38603723>

latent groups be compelled to act in a group oriented way.”⁹ He states that “in a large group in which no single individual’s contribution makes a perceptible difference to the group as a whole...it is certain that a collective good will not be provided unless there is coercion or some outside inducements that will lead the members of the large group to act in their common interest”.¹⁰

Contracted Parties are viewed as a “latent group” in the context of this study, as individual action—or inaction—regarding differentiation on the part of one Contracted Party does not affect *other Contracted Parties*. Should differentiation become a policy requirement, they would largely bear the risks and costs of differentiating RDDS data. However, the model provided at the end of this report aims to illustrate the effects of Contracted Parties mobilizing out of this “latent” state to provide differentiated RDDS data, and how this would impact not only Contracted Parties, but also registrants and RDDS end-users.

RDDS data are characterized as a “public good” in the context of this report. However, what constitutes a “public good” can be subject to interpretation. For example, some taxpayer groups may be willing to pay for more public goods (e.g. health care). However, another taxpayer group may view more spending in that same area as a burden, and detrimental to the public good of having the lowest possible tax rate. A similar perspective can be taken as it relates to differentiation. The increased amount of RDDS data that would be available under a differentiation policy would provide a public good to a large group of RDDS end-users and the constituencies they serve. On the other hand, the privacy protections contained within the GDPR and *Interim Policy* provides the public good of data privacy and ownership to data subjects. In the context of collective action theory, the GDPR represents a coercive incentive for data processors to provide these protections. The relative value of more RDDS data through differentiation must be evaluated against the relative value of ensuring registrants’ personal data remain protected to the fullest extent mandated by the GDPR.

⁹ Olson, *Logic of Collective Action*, p. 52.

¹⁰ *Ibid.*, p. 44.

Collective action theory helps frame the issue of differentiation in terms of group size and interests; but this study is not intended to test it. Rather, it is intended as an inductive tool to help the EPDP Team identify general principles as they relate to differentiation, with an aim to provide a balanced framework for the Team to compare the *status quo* against a hypothetical policy to differentiate. It applies Olson’s general research strategy to find and assert “stark and simplifying propositions”; that is “looking for the areas where there can be a breakthrough—for areas where strong claims are in order ... it is a good research strategy to search for stark and simplifying propositions.”¹¹

Research Questions

Recommendation 17.2 requests research into the costs, risks, and feasibility of differentiation. In its advice to the EPDP Team regarding the Recommendation, the ICANN’s Governmental Advisory Committee (GAC) noted that that “the Recommendation discusses only the risks and costs of this differentiation but does not mention the benefits of this distinction. Hence the GAC recommends that the study include an examination of the benefits of providing this information to the public.”¹² With these recommendations in mind, this report focuses on five key variables as they relate to differentiation: **Cost**, **Risk**, **Cost-Risk Mitigation**, **Benefits**, and **Feasibility**. As these variables are not amenable to quantitative measurement, the relationship between them cannot be rigorously tested without an expanded effort. To the extent they can be measured at all, they are presented in the model provided [below](#) as qualitative variables with relative weights. These weights are derived from a review of legal analyses and academic research presented in the first sections of the report, as well as the results of a questionnaire on differentiation circulated amongst the EPDP Team and ICANN Community.

The overarching questions guiding each aspect of the research effort are as follows:

¹¹ Oates, Wallace, Joe Oppenheimer, and Thomas C. Schelling. "In Memoriam: Remembering Mancur Olson." *Southern Economic Journal* 66, no. 3 (2000): 793-800. www.jstor.org/stable/1061440.

¹² ICANN GNSO (20 February 2019), Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process, p. 186.

1. What are the potential **risks** and **costs** of differentiation to ICANN Contracted Parties, registrants (“data subjects”), and end-users of RDDS data?
2. What factors work to mitigate those risks and costs?
3. What are the **benefits** of differentiation?
4. How do **mitigation** factors and the **benefits** of differentiation impact the **risks** and **costs** of differentiation?
5. What factors explain the relative **feasibility** of differentiation for each party?

Questionnaire

To gather insight into different practices and perceptions as they relate to differentiation, ICANN org circulated a short questionnaire targeted at members of the ICANN community representing five groups as part of its research for this report: 1) Contracted Parties; 2) Natural Person Registrants; 3) Legal Person Registrants; 4) RDDS End-Users; and 5) the ccTLD community. ccTLDs were included as a response group in the questionnaire as many have had experience implementing differentiation methods (see [below](#)). The questionnaire opened 24 February 2020 and closed on 31 March 2020. It consisted of 6 primary questions:

1. Why does your organization differentiate?
2. What methods does your organization use?
3. Why your organization does not differentiate?
4. Has your organization’s home jurisdiction impacted a decision to differentiate?
5. What are the perceived main benefits associated with differentiation?
6. What are the perceived risks and costs associated with differentiation?

The questionnaire received 247 responses. Respondents identified themselves as either a Contracted Party, legal person registrant, natural person registrant, RDDS end-user, or ccTLD operator. The proportion of responses per group is as follows:

- About half (47%) identified as a legal person registrants
- About a third (30%) identified as a registration data end-user
- 14% identified as a Contracted Party
- 4% identified as a natural person registrants
- 4% identified as a ccTLD Operator

Note the questionnaire was not designed to allow for any statistical inference from the responses; they are presented solely for their qualitative value in understanding the **risks**, **costs**, **mitigation** and **benefits** associated with differentiation. Responses are included as references throughout the report, and, to the extent applicable, inform the model presented [below](#).

Differentiation and the GDPR

In 2017, the Economist magazine declared that data had surpassed oil as the world's most valuable resource.¹³ As the amount and value of data on the Internet has increased, so has the “tension between data markets and privacy.”¹⁴ The personal data of individuals, or “natural persons,” are gaining stronger legal protections around the world, with the most notable example being the European Union's General Data Protection Regulation (GDPR).¹⁵ The GDPR has become a global standard for data protection, driven by what Bradford dubs “the Brussels Effect”: the de facto compliance with European regulations on the part of international firms who would otherwise find it too costly to operate separate systems for the EU and “everyone else”.¹⁶ About 120 countries have passed data protection laws that resemble it.¹⁷ Bradford argues this standardization occurs through a process of “unilateral regulatory globalization,” which happens when “a single state is able to externalize its laws and regulations outside its borders through market mechanisms, resulting in the globalization of standards.”¹⁸

The GDPR strengthens natural persons' control over their personal data. Subtitled “On the protection of natural persons with regard to the processing of personal data and on the free movement of such data”, its opening Recitals state: “the protection of natural persons in relation to the processing of personal data is a fundamental right...[and] the principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of

¹³ Economist (5 May 2017), “The world's most valuable resource is no longer oil, but data”, <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>

¹⁴ Economist (6 May 2017), “Data is giving rise to a new economy”, <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy>

¹⁵ In general legal terms, a “natural person” refers to “a human being, capable of assuming obligations and capable of holding rights”. See: Adriano, Elvia Arcelia Quintana. 2015. “The Natural Person, Legal Entity or Juridical Person and Juridical Personality.” *Penn State Journal of Law & International Affairs* 4 (1): 363 - 391. <https://elibrary.law.psu.edu/jlia/vol4/iss1/17> p. 366.

¹⁶ Bradford, Anu (2012), “The Brussels Effect”, *Northwestern University Law Review*, 107(1), https://scholarship.law.columbia.edu/faculty_scholarship/271

¹⁷ Economist (20 Feb 2020), “The EU wants to set the rules for the world of technology”, <https://www.economist.com/business/2020/02/20/the-eu-wants-to-set-the-rules-for-the-world-of-technology>

¹⁸ Bradford (2012), “Brussels Effect”, p. 3. Bradford notes the concept is derived from similar effects seen in federal systems such as the US, notably the “California Effect”. It describes how California, by far the largest internal market in the US, is able to set regulatory standards at the state level that translate into *de facto* national standards, since the costs of compliance with two standards are too high for most firms. Similarly, the “Delaware Effect” describes how the state of Delaware's incorporation process is relatively lax compared to other states, which incentivizes other states to adopt similar processes to attract corporations and the revenues they bring.

personal data.”¹⁹ It applies to any party that processes personal data within the EU or internationally on the part of EU citizens, and requires **consent** from data subjects in order to process any of their personal data.²⁰ However, it *does not* apply to the data of legal persons such as corporations (for- and non-profit), government bodies, educational institutions, non-governmental organizations, and other such entities endowed with “juridical personality” under their respective national laws.²¹

Well before the GDPR took effect, Kuner (2003) identified the central challenge of differentiation in *European Data Privacy Law and Online Business*, namely ensuring that the designation is accurate and does not contain personal data without consent to process it:

The extension of data protection law to legal persons gives rise to a variety of questions. For instance, it can be difficult to differentiate between the personal data of a natural person and a legal person, such as when the person is the sole proprietor of a small business. Generally speaking, courts will look behind the designation given to a particular data set in order to allocate it either to a person or a legal entity...[I]n Germany the courts have been willing to consider the data of a legal entity to be ‘personal data’ of a natural person, when data concerning the legal entity closely relates to a natural person (for example, data concerning a company could be used to identify the managing director of the company, and so might be considered to be ‘personal data’ of the managing director).²²

¹⁹ Regulation 2016/679 of the European Parliament and Council (General Data Protection Regulation) (27 April 2016), <https://gdpr.eu/tag/gdpr/>, Recitals 1 and 2. In Article 4(1), the GDPR defines personal data as “any information relating to an identified or identifiable natural person (‘data subject’), and a natural person as “one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”. In Recital 30, it lists further identifiers that could qualify as personal data: “Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.”

²⁰ Article 6 of the GDPR, “Lawfulness of processing”, states a number of requirements around how to process personal data. See: gdpr.eu, “Art. 6 GDPR: Lawfulness of processing”, <https://gdpr-info.eu/art-6-gdpr/>. For a summary overview of these requirements, see: “What is GDPR, the EU’s new data protection law?”, <https://gdpr.eu/what-is-gdpr/>

²¹ Recital 14 of the GDPR states: “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.” A legal person refers to “those entities endowed with juridical personality who are usually known as a collective person, social person, or legal entity.” See Adriano (2015), “Natural Person, Legal Entity or Juridical Person”, p. 366.

²² Kuner, Christopher, “Chapter 2: Fundamental Legal Concepts” in *European Data Privacy Law and Online Business*, (Oxford University Press, 2003), pp. 49-84.

At the time, Kuner noted that “not much attention [had] been given by courts and academic commentators to differentiation between the data of legal and natural persons in those countries where the personal data of legal entities is protected, so...there [was] a good deal of uncertainty.”²³ This uncertainty persists, and with uncertainty comes risk. A major violation of the GDPR can result in a fine of up to €20 million, or 4% of an organization’s total revenue. The highest fine to date was levied on British Airways in the amount of €204.6 million for “insufficient technical and organisational measures to ensure information security.”²⁴ However, statistics on fines resulting from GDPR enforcement show a wide range of financial penalties. The lowest fine displayed on enforcementtracker.com, which tracks fines levied as a result of GDPR enforcement, was €118 for “insufficient legal basis for data processing.”²⁵ Most of the fines listed on enforcementtracker.com are relatively small, ranging from a few hundred to a few thousand euros. A small proportion of them are much larger, and usually tied to high-profile, systemic violations committed by large firms.²⁶ In the EU, the data protection authority (DPA) of each member state determines whether a violation has occurred and the severity of the fine based on the following criteria:

- **Gravity and nature** — *The overall picture of the infringement. What happened, how it happened, why it happened, the number of people affected, the damage they suffered, and how long it took to resolve.*
- **Intention** — *Whether the infringement was intentional or the result of negligence.*
- **Mitigation** — *Whether the firm took any actions to mitigate the damage suffered by people affected by the infringement.*
- **Precautionary measures** — *The amount of technical and organizational preparation the firm had previously implemented to be in compliance with the GDPR.*
- **History** — *Any relevant previous infringements, including infringements under the Data Protection Directive (not just the GDPR), as well as compliance with past administrative corrective actions under the GDPR.*
- **Cooperation** — *Whether the firm cooperated with the supervisory authority to discover and remedy the infringement.*
- **Data category** — *What type of personal data the infringement affects.*

²³ Ibid., p. 58.

²⁴ enforcementtracker.com, “Fines Statistics: Highest fines: individual,” <https://www.enforcementtracker.com/?insights>.

²⁵ Ibid., “Fines Database,” <https://www.enforcementtracker.com/?insights>.

²⁶ enforcementtracker.com provides interactive fine models from Germany and the Netherlands to help parties determine what a potential fine could be. See “Fines Models by DPAs,” at <https://www.enforcementtracker.com/?insights>.

- **Notification** — Whether the firm, or a designated third party, proactively reported the infringement to the supervisory authority.
- **Certification** — Whether the firm followed approved codes of conduct or was previously certified.
- **Aggravating/mitigating factors** — Any other issues arising from circumstances of the case, including financial benefits gained or losses avoided as a result of the infringement.²⁷

Current Policy and Recommendations

ICANN’s Generic Names Supporting Organization (GNSO) initiated Phase 1 of the EPDP in July 2018 to determine whether the *Temporary Specification for gTLD Registration Data* (Temp Spec)--currently in effect as the *Interim Registration Data Policy for gTLDs*--could should become an ICANN Consensus Policy that complies with the GDPR and other relevant privacy and data protection legislation.²⁸ Under the *Interim Policy*, registrants must provide contact details for the registered name holder, and may provide those of any administrative (*Admin*) and technical (*Tech*) contacts.²⁹ If the registration data contains personal data in these latter fields, the contacts listed must also have provided consent to have their data processed for the purposes of the domain name registration.³⁰ As it relates to registration data requiring redaction under the *Interim Policy*, Contracted Parties may also provide an option for registrants to **consent** to have these data published in public RDDS.³¹ In its Phase 1 Final Report, the EPDP Team included the following as Recommendation 6: “as soon as commercially reasonable, Registrar[s] must provide the opportunity for the Registered Name Holder to provide its Consent to publish redacted contact information, as well as the email address, in the RDS for the sponsoring registrar.”³²

²⁷ gdpr.eu, “What are the GDPR Fines?”, <https://gdpr.eu/fines/>

²⁸ The *Interim Policy* requires Contracted Parties to continue following measures consistent with the *Temp Spec* until the *Registration Data Policy for All gTLDs* goes into effect. See: ICANN.org, *Interim Registration Data Policy for All gTLDs*, <https://www.icann.org/resources/pages/interim-registration-data-policy-en>. For the current status of the *Registration Data Policy* implementation, see: ICANN.org, “Registration Data Policy for gTLDs (EPDP Phase 1 Implementation),” <https://www.icann.org/resources/pages/registration-data-policy-gtlds-epdp-1-2019-07-30-en>.

²⁹ ICANN.org (25 May 2018), *Temporary Specification for gTLD Registration Data*, Appendix A: Sections 2.2 – 2.4.

³⁰ Ibid.

³¹ See Section 7.2 of the *Interim Policy*.

³² ICANN GNSO (20 February 2019), *Final Report on the Temporary Specification for gTLD Registration Data Expedited Policy Development Process*, p. 42.

In regard to differentiation, the *Interim Policy* states: “distinguishing between legal and natural persons to allow for public access to the Registration Data of legal persons, which are not in the remit of the GDPR,” remains an outstanding issue for ICANN Community discussions.³³ In its Phase 1 Final Report, the EPDP Team recommended that a provider of domain name registration services *may* differentiate according to whether the registrant is a legal or natural person, but is not obligated to do so.³⁴

³³ Ibid., Annex, p. 32, pt. 5.

³⁴ Recommendation 17.1. See: ICANN GNSO (20 February 2019), *Final Report on the Temporary Specification for gTLD Registration Data Expedited Policy Development Process*, p.17. For the charter questions guiding the EPDP Team’s deliberations on differentiation, see: “Charter for the Temporary Specification for gTLD Registration Data EPDP Team” (19 July 2018), <https://gns0.icann.org/sites/default/files/file/field-file-attach/temp-spec-gtld-rd-epdp-19jul18-en.pdf>. They included: “h3) Should Contracted Parties be allowed or required to treat legal and natural persons differently, and what mechanism is needed to ensure reliable determination of status?”; “h4) Is there a legal basis for Contracted Parties to treat legal and natural persons differently?”; and “h5) What are the risks associated with differentiation of registrant status as legal or natural persons across multiple jurisdictions?”

Differentiation: Problems and Prospects

Prior to the GDPR's effective date, ICANN org engaged with the (now disbanded) Article 29 Data Protection Working Party (WP29) for advice on how to handle RDDS data under the GDPR. WP29 stated a general rule on processing data to comply with the then forthcoming Regulation: "A central consideration ... is that the data subject should be able to determine in advance what the scope and consequences of the processing entails ... they should not be taken by surprise at a later point about the ways in which their personal data has been used."³⁵ Differentiation raises the prospect of "surprising" data subjects—i.e. registrants—with unintended processing of their data. For example, if a natural person registrant was incorrectly designated as legal person, his/her personal data may be published in public RDDS. This raises a risk—and potential cost—for both the data subject and processor: the data subject's privacy is at risk, which may impose costs on him/her, and the data processor faces a liability risk under the GDPR if it does not have the legal basis to process the registrant's personal data. A number of respondents to the questionnaire representing Contracted Parties noted that—in the absence of a reliable differentiation mechanism—they treat all RDDS data from registrants as if they contain personal data, either to comply with the GDPR or because they have no obligation to differentiate:³⁶

"We decided to treat all [registration data] the same way to comply with GDPR."

"Neither us nor our clients had any obligations to differentiate and there was no policy around this, so all the data is effectively treated the same."

"Applying a uniform approach to data redaction is in the best interest of our customers. There is no current mechanism that allows us to reliably distinguish between Legal and Natural persons registrants."

³⁵ Article 29 Data Protection Working Party (11 April 2018), *Guidelines on Transparency under Regulation 2016/679*, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227, p. 7.

³⁶ Bird & Bird LLP (25 January 2019), "Memorandum to ICANN org and EPDP Team: Advice on liability in connection with a registrant's self-identification as a natural or non-natural person pursuant to the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') EPDP Wiki: Legal Memos and Input: Natural vs. Legal Memo.docx. <https://community.icann.org/display/EOTSFGRD/EPDP+Small+meeting+on+Legal+Committee+Framework>.

“[Differentiation has] never been a requirement.”

However, a respondent to the questionnaire provided a contrasting view, contending that legal person data should *not* be grouped with personal data in RDDS: “It appears very clearly that only personal data of individual domain name holders are requested to be protected and undisclosed in the WHOIS. Not distinguishing between legal and natural person is a misinterpretation of European [Data Protection Authorities’] explicit recommendations on the new legal framework.” This view echoes that of ICANN’s Governmental Advisory Committee (GAC), which contends that non-differentiation as currently practiced by many Contracted Parties—i.e. treating all registration data as personal—exceeds the scope of the GDPR as it does not cover the data of legal persons.³⁷ This illustrates a fundamental tension between groups advocating for the interests of the RDDS end-user community, who face risks and costs if RDDS data are *not* differentiated, and Contracted Parties, who would bear the “burden” of differentiation—i.e. the risks and costs associated with implementing a differentiation method.

³⁷ ICANN GAC (20 February 2019), Governmental Advisory Committee¹ Input on the Draft Final Report of the Expedited Policy Development Process (EPDP) on gTLD Registration Data, <https://gac.icann.org/publications/public/epdp-draft+final-report-revised+gac-input-20feb19-final.pdf>.

Risks and Costs: The Burden of Differentiation by Party

Contracted Parties

For Contracted Parties to differentiate, they would need to implement methods to accurately identify a registrant as a legal or natural person, as well as ensure that any legal person RDDS data does not contain the personal data of employees (unless those employees have provided their explicit consent to have their data processed for the purposes of the domain name registration). The expense of any such methods, while difficult to determine specifically, would amount to a cost for Contracted Parties; they would likely need to integrate a number of fixed and/or variable costs into their operating expenses associated with verifying the designation and ensuring they maintain all necessary consent records. As two questionnaire responses noted:

“...from a development standpoint, the cost of implementing the state of the art, or best practice technology to enable differentiation would be significant.”

Future costs will come from re-engineering well-vetted and use-tested systems to add the ability to capture this fairly useless data, re-engineering and redesigning website, customer portal, support tools, and other systems to capture and update this data. The support calls and customer service issues related to walking through the typical human being on understanding what legal vs natural means. If the capture of this and its accuracy become mandatory, the costs of staff and audit, plus customer outreach to force revision of the information will be expensive.

The EPDP Team discussed two potential methods to differentiate. A registrant could *self-identify* as a legal or natural person—or provide a proxy indicator as discussed [below](#)—or the Contracted Party (or designated third-party) could make the determination.

Registrant Self-Differentiation

Self-identification would obviate the need for more complex mechanisms to differentiate. When asked how differentiation is/should be carried out, some respondents indicated self-identification was a sufficient measure:

“Self-declaration as for any other data submitted by our customers”

“A simple legal vs. natural flag that enables publication or redaction according to the registrant's self-assertion should suffice.”

However, relying on registrant self-identification poses a risk to Contracted Parties and to natural person registrants should registrants “not understand the consequences of what would seem to be a technical designation.”³⁸ For example, a registrant running a small online company from his/her home as a sole proprietor may be a legal person, but may not want his/her home address publicly available in RDDS. Contracted parties could be subject to liability if this registrant were to incorrectly self-identify, and the registrant's personal data were disclosed based on this self-identification.³⁹ Several respondents to the questionnaire noted the challenges of self-differentiation to Contracted Parties:

“It is too hard as often even the data subject is using a wrong self-declaration. The lines between private persons and companies can be quite blurred (i.e. under German company law a company name of a person company is the first and last name of the company owner) I why [sic] we decided to treat all data as if it would private data”.

We do not differentiate because we can't reliably verify the accuracy of the assertion by the data subject. In addition, in line with legal guidance received by the EPDP, that presents a high level of risk to the data subject as well as to the contracted party. Further, putting the onus on the registrant to make the determination between legal and natural can be difficult based upon the situation (i.e. a natural person registering a

³⁸ Bird & Bird LLP (25 January 2019), “Natural vs. Legal Memo”, p. 4.

³⁹ Ibid.

domain for a legal entity and including their personal data in a registration) and could lead to the accidental exposure of personal data, or legal entities being improperly identified.

“IF accuracy of this field is something that becomes mandated, the confusion that most registrants have had over filling out similar captured fields beyond an address and telephone number with .US or .UK domain registrations have indicated that this will never be perfect”

Differentiation by Contracted Party

Rather than rely on a registrant’s self-identification as a legal or natural person, Contracted Parties could implement methods to designate a registration as that of a legal or natural person on their end. However, differentiation carried out by Contracted Parties carries its own set of risks: if they were to make a mistake with a designation—a distinct possibility given the scale on which many operate—they could face liability risk if personal data are processed as those of a legal person. If a Contracted Party uses a third party to process its data, and that party processes personal data as legal person data, the Contracted Party would still be liable for any GDPR violations that occurred as a result (as would the third party).⁴⁰ One questionnaire respondent identified the possibility of a violation as a result of an incorrect designation:

“The risk is that if personal data might be incorrectly disclosed to the general public due to it being classified as relating to a legal person then that could lead to complaints and ultimately sanctions under GDPR.”

Another respondent summarized the challenges of both registrant self-identification and differentiation by Contracted Parties:

Registrant self-identification (as a Legal or Natural person) carries a risk that registrants will misidentify, leading to the inadvertent publication or redaction of their personal data. Moreover, even Legal person registration data may contain Natural person data (e.g., Tech or Admin Contact), and in our view there are not sufficient mechanisms to validate that consent obtained by the Legal person registrant on behalf of a natural

⁴⁰ gdpr.eu, “What are the GDPR Fines?”

person may be relied upon by Contracted Parties as a basis for publishing data. As a result, the transfer of both consent and withdrawal of consent up the chain of parties (i.e., from natural person to Legal person registrant to registrar to registry) pose significant legal and technical challenges. In light of the risks involved in the publication of personal data in violation of global data protection laws, at this time we prefer to treat Legal and Natural person registrants the same, although we appreciate the flexibility to make that determination on our own as we see fit.”

This respondent identified an important nuance hindering a “down the middle” separation of legal and natural persons in RDDS: legal person registration data may contain the personal data of natural persons associated with the legal person registrant. Bird & Bird provide a useful example: if a business were to register a domain name and provide contact details associated with a natural person—e.g. *firstname.lastname@company.example*—those data would be considered personal. According to Bird & Bird, publishing them in the public RDDS without proper consent would be a violation of the GDPR. However, providing the generic contact details of the company--e.g. *info@company.example*--would not be.⁴¹ This is particularly relevant to the *Admin* and *Tech* fields of RDDS data; legal person registrants are more likely to enter information in these fields given the generally larger scale of their online operations. If these fields contain any personal data, both the registrant and the registrar must ensure that those data are either processed as personal data, or that the contacts in those fields have provided consent to the primary registrant to process their personal data as part of a legal person registration. If an organization were to register a domain name as a legal person, and the registration data it provided to its registrar contained the personal data of its associates obtained without their informed consent, the registrar could face a liability risk—along with the legal person registrant—if that data was made public or otherwise used without the data subjects’ informed consent.⁴² This illustrates a key issue with differentiation as currently conceived: *legal person registration data cannot automatically be processed as non-personal data*. As noted in its 5 July 2018 letter to ICANN org, the European Data Protection Board (EDPB) stated: “The mere fact that a registrant is a legal person does not necessarily justify unlimited publication of personal data relating to natural persons who work for or represent that organization, such as natural persons who manage the administrative or technical issues on behalf of the registrant.”⁴³

⁴¹ Ibid.

⁴² Bird & Bird LLP (25 January 2019), “Natural vs. Legal Memo”, p. 2.

⁴³ Jelinek, Andrea (5 July 2018), “Letter from Andrea Jelinek, Chairperson, European Data Protection Board Chairperson, to Goran Marby, ICANN Org CEO”, <https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf>

Data Subjects

Natural Person Registrants

Natural person registrants face a risk to their privacy should their registration data be processed as those of a legal person. In the event their personal data are processed incorrectly, the costs to natural person registrants could vary widely. For example, if their personal data are published in RDDS, the registrant may get annoying spam or robocalls. In extreme cases, the natural person's online presence and physical safety could be at risk should a malicious actor exploit the registrant's data to engage in more serious criminal activity. One questionnaire respondent noted the risk of differentiation to natural person registrants as the "incorrect application of categorization that exposes natural persons data inappropriately particular [sic] when domains switch between the different types by transfers/acquisitions". Another stated potential political risks to natural person registrants who use their domains as platforms for activism: "Natural person risk maybe in terms of oppressive governments having access to opposition critical identity [sic]."

While some natural person respondents indicated risks to their interests, others described the utility of accessible RDDS data, and why legal and natural persons should be treated differently in terms of registration data processing:

"I believe that in the case of natural persons confidentiality is prevailing over transparency while this is not necessarily the case for legal persons. Also, as a user, I would like to be able to access data about organizations (legal persons) with whom I may engage in commercial transactions."

"Legal persons are corporations formed for the purpose of selling something or conducting other business. For the purposes of ethical business transparency, they should not have the same privacy right as individuals."

Legal Person Registrants

For legal person registrants, risks and potential costs arise from the possibility of submitting associates' personal data—especially in RDDS *Admin* and *Tech* fields as noted [above](#)—to a Contracted Party without the proper consent. If *any* registrant provides information in these fields, he/she must ensure that the information either does not contain personal data, or if it does, that it was obtained and submitted for processing to a Contracted Party with the informed consent of those contacts. One respondent from the questionnaire noted this as a challenge:

“Beyond the technical difficulty of differentiating between person types, data relating to a Legal person has a high likelihood of also including identifiable information about a Natural person, and so should be afforded the same privacy protections”.

RDDS End-Users

For the most part, questionnaire respondents representing this group argued that the decreased availability of RDDS data under the *status quo* imposes a collective cost on the RDDS end-user community. The primary risks and costs of differentiation to RDDS end-users appear to be collective, dependent on the scope of end-users' work with RDDS data, and, in general, stem from *not* differentiating. For example, some end-users may use RDDS data for domain investing and speculation, while others use them to combat DNS abuse and intellectual property infringement. Fewer RDDS data would impact both groups. However, in the case of the former, access to fewer data negatively impacts the commercial operations of a niche industry; the risks and costs in that case are concentrated. For the latter, access to fewer data may impact the health of the DNS overall; the risks and costs in that case are distributed.

A number of respondents to the questionnaire provided detailed views:

Additional cost risks [sic] identified were costs that would likely fall on IP and law enforcement entities due to the data being redacted or unavailable to conduct their line of work. For example if a natural person registers for a domain their data will automatically be hidden due to laws such as GDPR, and there is a likelihood that DNS abuse takes place under such domains. Therefore, authorities would most likely incur

costs as they will need to reach out to registrars and registries to provide disclosed information based on legal bases. Costs will be incurred per complaints that need to be filed such as URDP or criminal proceedings.

“Differentiation between legal and natural persons in RDDS could, from the law enforcement authorities’ perspective, cause greater complications in criminal proceedings. It could also have the effect of increasing costs for law enforcement authorities because of the need to obtain the information needed for criminal proceedings via another (more costly) way.”

“The main risk and/or costs associated with the differentiation between Legal & Natural Persons is the investigation of registrations and the creation of complaints.”

“If there was no differentiation then all Registrant data would need to be redacted in the same way. This is not required under GDPR and it would significantly hamper attempts by IP rights owners to police infringements on the internet.”

“There are increased costs and time spent on requesting registration information from registrars and creating needless complaint documents such as UDRP complaints, Cease & Desist Letters, etc.”

“the countless domains registered with malicious intent costs us time and money to pursue, as more often than not, these are individuals (natural persons) and not legal organizations.”

“The transfer of costs to third parties (Law and IP enforcement agencies) flows into the second risk participants identified where differentiation between legal and natural persons may impact and hinder the work of agencies that protect the domain name industry from abuse.”

“From the point of view of legal subject, many domain name will be registered with bad faith under the name of natural person if the natural person’ information is overprotected. It will also cause inconvenience for regulation and maintain of government and enterprises. We used to fighting against the natural person who have many domain names in suspect of infringement while we have to do it one-by-one now.”

“The main risks for a company is that if a natural person is masked on the Whois, we cannot identify him and take the necessary legal actions. Consequently, we have to systematically file complaints instead of solving the case amicably.”

“If the registrant is a natural person, there may be more registrations made by this party that we cannot identify. This is a waste of cost & time as we would have to file one complaint for each registration found vs. one complaint per respondent. This affects both us internally and the WIPO Administration / local court ends for both cost & time issues. The registrar and internal time spent on transfers for successful recoveries should also factor into the time and cost wastes.”

However, some respondents noted an increased risk of legal person registrants designating themselves as natural persons to exploit privacy protections given to natural persons under the GDPR. These protections could be exploited by unscrupulous organizations to engage activities such as DNS abuse, IP infringement, and cybersquatting, which could in turn negatively impact domain security and consumer trust. These respondents tended to stress that registration data for legal entities should be made available:

“What we see is that natural persons register domain names that would be used by legal persons (their own company, for instance). Persons engaging in unlawful activities will certainly try to exploit the protection of natural persons’ WHOIS data to make the job of LEAs or IP holders more difficult. We therefore encourage the creation of a system that would make this difficult, if not impossible.”

“[A] Huge downside of the current ICANN GDPR situation is, that infringers get away with everything online although naturally nowadays, the businesses are shifting from the offline world to the online world. Consumers get confused, betrayed by the infringers and risk their health by being flooded with counterfeit products because right owners cannot find out who is the company behind the fraudulent site.”

A legal entity to me should have to have their domain Whois publicly available. A natural person should be able to choose whether they want to have their information available for their domain Whois. Considering however that anyone can register a domain name and claim it is a legitimate business even if it is not a legal entity allows fraudsters to continue to register and have their domain Whois information masked. Even when a domain is registered the information that is provided is often not vetted. For example, the registrant information can be empty or just filled in because the sole purpose of creating the domain was for fraudulent purposes: telephone numbers are invalid, addresses are invalid, and/or email addresses - assuming they are even legitimate - will not go answered by the registrant.

Easing the Burden of Differentiation: Methods to Mitigate Risks and Costs

Contracted Parties

Consent to Process Registration Data

Obtaining and recording the proper **consents** to process RDDS data—especially as it relates to data availability in public RDDS—may reduce some risk associated with differentiation to Contracted Parties.⁴⁴ Contracted Parties may provide an option for registrants to consent to have data that would otherwise be redacted published in public RDDS.⁴⁵ This reduces the risk of unintentional data publication, as all registrants provide consent for how their data is treated by default. The EPDP Team recommended this policy be continued in Recommendation 6 of their Final Report: “... as soon as commercially reasonable, Registrar must provide the opportunity for the Registered Name Holder to provide its Consent to publish redacted contact information, as well as the email address, in the RDS for the sponsoring registrar.”⁴⁶

However, both the GDPR and *Interim Policy* mandate that data subjects must be able to withdraw consent freely at any time.⁴⁷ In *Guidelines on Consent under Regulation 2016/679*, WP29 stated: “if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent.”⁴⁸ The *Interim Policy* accommodates this requirement by

⁴⁴ Recital 32 of the GDPR details requirements for consent: “Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.”

⁴⁵ See Section 7.2 and Appendix A: Sections 2.2 – 2.4 of the *Temporary Specification for gTLD Registration Data* (25 May 2018).

⁴⁶ ICANN GNSO (20 February 2019), *Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process*, p. 8.

⁴⁷ See Article 7.2, *General Data Protection Regulation* (27 April 2016), “Art. 7 GDPR: Conditions for consent,” <https://gdpr.eu/article-7-how-to-get-consent-to-collect-personal-data/> and Provision 7.2.3 of the *Temporary Specification for gTLD Registration Data* (25 May 2018).

⁴⁸ Article 29 Data Protection Working Party (10 April 2018), *Guidelines on Transparency under Regulation 2016/679*, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

allowing registrants to withdraw their consent, but states specifically: “the withdrawal of Consent SHALL NOT affect the lawfulness of Processing based on Consent obtained before the withdrawal.”⁴⁹

The EPDP Team requested external legal guidance on how to treat consent as it relates to the RDDS data of individuals other than the Registered Name Holder (RNH), specifically those contained in RDDS *Admin* and *Tech* fields. As it relates to differentiation, a legal person registering a domain name could provide consent to a Contracted Party to process RDDS data containing the personal data of associates without obtaining the proper consent. In a 5 July 2018 letter to ICANN org, the European Data Protection Board (EDPB), advised: “it should be ensured that the individual concerned is informed” if contact details for persons other than the RNH are provided for the registration.⁵⁰ The EPDP Team discussed whether this advice implied that it is sufficient for the RNH to inform the individual it has designated as the *Admin* or *Tech* contact, or whether the registrar may have additional legal obligations to obtain consent.

The EDPB provided the following clarification, and suggested two means to mitigate issues associated with obtaining consent from individuals other than the RNH:

...registrants should in principle not be required to provide personal data directly identifying individual employees (or third parties) fulfilling the administrative or technical functions on behalf of the registrant. Instead, registrants should be provided with the option of providing contact details for persons other than themselves if they wish to delegate these functions and facilitate direct communication with the persons concerned. It should therefore be made clear, as part of the registration process, that the registrant is free to (1) designate the same person as the registrant (or its representative) as the administrative or technical contact; or (2) provide contact information which does not directly identify the administrative or technical contact person concerned (e.g. admin@company.com). For the avoidance of doubt, the EDPB recommends explicitly clarifying this within future updates of the Temporary Specification.⁵¹

⁴⁹ Temporary Specification for gTLD Registration Data (25 May 2018), Provision 7.2.3.

⁵⁰ Jelinek, Andrea (5 July 2018), “Letter from Andrea Jelinek, Chairperson, European Data Protection Board, to Goran Marby, ICANN Org CEO”, footnote 15.

⁵¹ ICANN GNSO (20 February 2019), *Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process*, p. 39.

A Data Processing Impact Assessment (DPIA) represents another mechanism that may work to mitigate some risks and potential costs of differentiation.⁵² Article 35 of the GDPR states: “Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.”⁵³ A DPIA provides an avenue for Contracted Parties to record any precautionary measures they have taken to mitigate potential issues associated with how they differentiate RDDS data. As noted [above](#), DPAs account for such measures in their assessment of whether a violation has occurred and the severity of the penalty if so.⁵⁴

In his blog “How to: GDPR, consent and data processing”, Olejnik (2018) offers detailed advice on a process to obtain and demonstrate consent for data processing. He summarizes his advice as follows:⁵⁵

- 1. Look at how consent is processed in your organization. Is the process in-line with GDPR? If no, consents must be recollected*
- 2. There’s no consent process in your organization? Chances are you aren’t meeting the previous point*
- 3. You process based on consent but you don’t have consents? Seems you don’t have any process in your organization at all. Build it. Recollect consents. In this order.*

⁵² gdpr.eu, “How to conduct a Data Protection Impact Assessment”, <https://gdpr.eu/data-protection-impact-assessment-template/>. gdpr.eu references the DPIA template provided by the United Kingdom’s Information Commissioner’s Office (ICO) as a guide to conducting a DPIA. See: UK ICO (9 February 2018), “Sample DPIA Template”, <https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf>

⁵³ *General Data Protection Regulation* (27 April 2016), “Art. 35 GDPR: Data protection impact assessment,” <https://gdpr.eu/article-35-impact-assessment/>

⁵⁴ gdpr.eu, “What are the GDPR Fines?”

⁵⁵ Olejnik, Lukasz (2 January 2018), “How to: GDPR, consent and data processing”, <https://blog.lukaszolejnik.com/how-to-gdpr-consent-data-processing/>

4. *How to design consent messages/prompts, and how to make sure the user has understood what it all means - this is a matter of consent engineering*

Accuracy of Legal v. Natural Person Designation in RDDS

Article 5(1)(d) of the GDPR states that personal data must be “accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay”. An incorrect designation as a legal or natural person would render a registrant’s data inaccurate—whether provided by the registrant or assigned by a registrar—thus raising the prospect of violating both the GDPR and ICANN Contracts and Consensus Policies.⁵⁶ Verifying a designation to ensure its accuracy involves numerous practical difficulties associated with verifying the data provided by millions of registrants spread across many global jurisdictions.⁵⁷ While accurate designations would decrease the risks associated with differentiation, the practicalities of ensuring the data are accurate would likely result in increased costs associated with domain name data management, and thus may impact the feasibility of implementing a differentiation method for Contracted Parties.

However, as with consent, having a record of the steps taken to ensure data accuracy—e.g. in a DPIA—may work to mitigate costs associated with an incorrect designation resulting in GDPR infringement. DPAs would account for this record in determining whether a violation occurred and the severity of any fine.⁵⁸ The United Kingdom’s Information Commissioner’s Office noted four key guidelines for organizations that regularly work with personal data under the jurisdiction of the GDPR:⁵⁹

1. You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.

⁵⁶ Note Recommendation 4 from the EPDP Team’s Final Report: “The EPDP Team recommends that requirements related to the accuracy of registration data under the current ICANN contracts and consensus policies shall not be affected by this [registration data] policy.” ICANN GNSO (20 February 2019), *Final Report on the Temporary Specification for gTLD Registration Data Expedited Policy Development Process*, p. 7.

⁵⁷ See ICANN.org, “WHOIS Accuracy Reporting System (ARS) Project Information,” <https://whois.icann.org/en/whoisars>

⁵⁸ gdpr.eu, “What are the GDPR Fines?”

⁵⁹ UK ICO, “Principle (d): Accuracy,” <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>

2. You may need to keep the personal data updated, although this will depend on what you are using it for.
3. If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
4. You must carefully consider any challenges to the accuracy of personal data.

The advice noted further: "[w]hat is a 'reasonable step' will depend on the circumstances and, in particular, the nature of the personal data and what you will use it for"; and that data controllers may need to enlist third-party services to independently verify the accuracy of the data.

The EPDP Team solicited advice from legal advisory firm Bird & Bird on whether Contracted Parties could be subject to liability under the GDPR if they were to rely on registrant self-identification as an accurate means to differentiate. The firm addressed questions from the Team on the implications of some registrants mistakenly self-identifying as "non-personal" registrants, even if either they are registering as a natural person or they provide personal contact details on behalf of a corporate entity.⁶⁰ Bird & Bird suggested that Contracted Parties could reduce some risk associated with differentiation "by either improving the accuracy of the registrants' self-identification or by introducing measures to independently verify the selection -- or both."⁶¹

Several respondents to the questionnaire suggested methods to mitigate some of the risks and costs of differentiation, which include auditing the designations contained in the registration data controlled by a Contracted Party, relying on self-designation, presenting clear language on the consequences of an incorrect designation to registrants, and alerting registrants if a party is requests their registration data:

A solution could be that registries conduct random checks among their (theoretically) 'natural registrants', in order to verify that they are indeed natural persons, with monthly reports being sent to ICANN about these checks. 'Natural registrants' whose domain names would clearly be

⁶⁰ Bird & Bird LLP (25 January 2019), "Natural vs. Legal Memo".

⁶¹ Ibid., p. 3.

used by legal persons or for the benefit of legal persons (even if the aim or activity is lawful) should be asked by registries that the domain name be registered again by said legal persons. Sanctions should be available for registrants refusing to comply, which could go as far as domain name deletion.

...a better solution is more clear disclosure and public education. If natural persons need to be 'cared for', it's because the industry has not performed its duty to inform the public properly. Registrants are not dumb. The industry should require that all registrants, as part of registering a domain name, be clearly notified that their information will be public unless they request privacy service, that will (1.) create opportunity for registrars and, (2.) allow the DNS to be used to stop crime and mal-intent, what it was meant to do since its creation [sic].

“There should be avenues to pierce those protections when the subject party (either legal or natural person) is accused of acting in bad faith or in violation of the good faith rights of another party.”

“End users should always provide government issued ID to their registrar to register a domain.”

“For Contracted Parties, it seems clear that a registrant should be able to make an informed self-selection as to whether it is a legal person or a natural person, with knowledge of the applicable consequences of its decision.”

“If a registrant is in doubt or is interested in concealing its identity, it seems to be of low or no risk to the Contracted Party to rely on the registrant's self-selection”

“If the options and the consequences are clearly presented (at minimal cost to the registrar) to the registrant, there is no cost or risk to registrants.”

“I would prefer that I am at least notified that someone is requesting to view my registration data”.

Data Subjects

Natural and Legal Person Registrants

Registrants, as data subjects, can do little to directly mitigate the systemic risks and costs associated with differentiation. They do have the option to utilize a privacy/proxy service to mask their registration data on an individual basis.

RDDS End-Users

If RDDS data were differentiated at scale and made available in public RDDS, RDDS end-users would benefit from the increased availability of registration data. As beneficiaries, RDDS end-users would have few costs and risks to mitigate in such a scenario.

Collective Mitigation Efforts

The EPDP Team is currently discussing a “System for Standardized Access/Disclosure” (SSAD) to non-public gTLD registration data.⁶² The aim is to define a system in which only vetted, legitimate interests—e.g many RDDS end-users—could access non-public gTLD registration data. However, building such a system is fraught with many substantive and idiosyncratic challenges beyond the scope of this report. If a reliable system could be defined, it may work to mitigate some of the issues associated with differentiation. Currently the SSAD project remains under discussion.

As a historical note, a number collective, technical standards for processing data to help comply with evolving data protection laws around the world have been proposed. In 2006, Weitzner, Hendler, and Berners-Lee argued that, “for all of the Web's success at meeting communication and information exchange goals, it has failed in equal measure at satisfying other critical policy requirements such as privacy protection, a balanced

⁶² ICANN GNSO (7 February 2020), *Initial Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process*, <https://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-initial-report-07feb20-en.pdf>, p. 9.

approach to intellectual property rights, and basic security and access control needs.”⁶³ Their research focused on the development of a “policy aware web.” It illustrated a transition from “role-based authentication” to “rule-based access policies”, in which “a declarative set of rules is used to define finer-grained access to resources with requests for data providing a ‘demonstration’ that they satisfy the policy encoded in the rules.”⁶⁴ With this in mind, the Internet community put forth a number of initiatives intended to standardize data protection and collection practices on the part of data processors. For example, the (now obsolete) Platform for Privacy Preferences (P3P) protocol aimed to provide a technical standard by which data processors could present privacy policies to data subjects and collect relevant personal and/or business information. Importantly, the protocol could be modified to present policies and request data in accordance with applicable data protection law.⁶⁵ The Transparent Accountable Datamining Initiative (TAMI) sought to develop “precise rule languages that are able to express policy constraints and reasoning engines that are able to describe the results they produce.”⁶⁶ Weitzner et al. (2006) noted the research in this area focused on developing technical capabilities to “specify access policies that don’t have to be defined in advance, have fine grained access, and allow fairly dynamic change.”⁶⁷ While these initiatives have not garnered the global support needed to implement them at scale, they do provide instructive examples of potential data processing standards that can be modified to comply with evolving data protection law around the world, and thus could serve to mitigate many of the problems of differentiation.

⁶³ Weitzner, Daniel J., Jim Hendler, Tim Berners-Lee and Dan Connolly (2006), "Creating a Policy-Aware Web: Discretionary, Rule-Based Access for the World Wide Web." In *Web and Information Security*, eds. Elena Ferrari and Bhavani Thuraisingham, doi:[10.4018/978-1-59140-588-7.ch001](https://doi.org/10.4018/978-1-59140-588-7.ch001), pp. 1 - 31.

⁶⁴ Ibid.

⁶⁵ Ramnath Chellappa, Ravinder Dharmapuram, and Rahul Hampole (22 April 2006), “Dynamic Privacy Enforcer: A Trusted Third-party Framework to Provide Personalization in the Presence of Privacy Concerns”, *Proceedings of the CHI2006 Workshop on Privacy-Enhanced Personalization*, Montreal, <http://isr.uci.edu/pep06/program.html>, pp. 16 - 20. See also: w3.org (2 February 2018), “Platform for Privacy Preferences (P3P) Project”, <https://www.w3.org/P3P/Overview.html>

⁶⁶ Massachusetts Institute of Technology, Computer Science and Artificial Intelligence Laboratory (2 February 2009), “Transparent Accountable Datamining Initiative”, <http://dig.csail.mit.edu/TAMI/>

⁶⁷ Weitzner et al. (2006), "Creating a Policy-Aware Web", p. 10.

Benefits: RDDS as a Collective Good

The benefits of differentiation can be viewed as a “collective good”: it may benefit a significant proportion of Contracted Parties, registrants, and RDDS end-users. However, as with any collective good, a small segment of the population bears the cost of providing it, while a larger segment of the population enjoys the benefits. A relatively small population segment providing a collective good for all means that segment is incurring proportionally larger **costs per capita** than the proportional value of the **benefits per capita**. In other words, some bear the cost of a collective good, while those who incurred little to no cost providing it enjoy the benefits.⁶⁸

Several respondents to the questionnaire suggested the benefits of differentiation involve the provision of a collective good, and are distributed among important RDDS end-user constituencies such as law enforcement, cybersecurity professionals, and intellectual property interests. The primary benefits of differentiation suggested by these respondents can be summarized as “security,” “authenticity,” and “transparency”:

“All commercial/organisational use of domains should be transparent for security and confidence of end users. Differentiating natural persons is helpful for the purposes of privacy regulations, although data should be accessible under certain circumstances (e.g. to respond to DNS Abuse activities).”

A legal entity to me should have to have their domain Whois publicly available. A natural person should be able to choose whether they want to have their information available for their domain Whois. Considering however that anyone can register a domain name and claim it is a legitimate business even if it is not a legal entity allows fraudsters to continue to register and have their domain Whois information masked. Even when a domain is registered the information that is provided is often not vetted. For example, the registrant information can be empty or just filled in because the sole purpose of creating the domain was for fraudulent purposes: telephone numbers are invalid, addresses are invalid, and/or email addresses - assuming they are even legitimate - will not go answered by the registrant.

⁶⁸ Olson, Mancur (1971), The Logic of Collective Action.

“Trademark enforcement, other patent opportunities”

“Differentiating between Legal and Natural persons works to prevent disputes between individuals/employees and the Legal entity with ultimate control over the domain name registration.”

“The domain name registration data for legal entities should remain available for the public. Such data is very important for law enforcement to protect the human rights for people being victims of crime and also to prevent actions of crime.”

“Differentiating between legal and natural persons will provide the basis for disclosing the registration data of legal entities which is not protected under the GDPR. Such information is important for consumer protection, law enforcement and cyber security professionals as they work to keep the internet safe for its users.”

“We are also a brand owner that must enforce its brands and that has been made much more difficult by the masking of registrant data in Whois due to GDPR. Any effort to increase the availability of registrant data, even if only the data of certain registrants (e.g., legal persons) would be highly beneficial.”

We also believe this solution to be logical and coherent. We are convinced that the GDPR is a major achievement for the protection of privacy on the Internet, which must be upheld and properly applied. However, we think that it is not in the spirit of the GDPR to anonymize the data of legal persons. What’s more, it is widely accepted that legal persons must submitted to a certain degree of transparency ‘in real life’ to be created and allowed to conduct their activities. Indeed, in almost all countries, legal persons, especially companies, must provide information that is made publicly available (identity of its managers and officers, address...) or sent to State administration (yearly accounts...).

Transparency is widely expected ‘IRL’ from legal persons, especially to foster trust and consumer information, and we see no reason why these

transparency rules should not apply to WHOIS data. In fact, the anonymity that is granted by the Internet should even render online transparency obligations greater for legal persons than they are 'IRL'.

In our view, the primary benefit of differentiating between legal and natural persons would be a significantly improved balance with regard to the regulation and oversight of commercial activity on the internet. Historically, consumers and other interested parties (e.g., owners of intellectual property) have been provided some ability to know with whom they are engaging in a business transaction. Nearly every jurisdiction in the world provides some legal framework for the registration of parties engaged in commercial operations – including an opportunity for relevant parties to access that information in a reasonable manner. The rules currently applicable in the e-commerce context, however, have substantially limited such abilities. The relative anonymity allowed for individuals selling goods online – including counterfeit or substandard goods which may harm consumers health and safety - and the substantial impediments to consumers' and other stakeholders' ability to access that information, allows bad actors to operate with impunity. Providing a distinction between natural persons and legal persons, and making the registrant data of those latter parties (who are more likely to be engaged in commercial activity online) would be a significant step towards addressing these concerns.

As a right holder, we use registration data to investigate the existence of an infringement to our intellectual property rights, as well as the risk of an attack on our systems (e.g.: registration of an IDN homograph domain). We also use the registration data for retrieving further infringing domains registered by the same infringer and/or attacker (e.g.: in view of an UDRP). Finally, we use the registration data to liaise with the infringer and offer to solve the matter amicably. Our observation is that the vast majority of infringements we investigated were committed by criminal organizations, as opposed to natural persons. And we generally do not believe that it is anyone's best interest to give up a chance to solve a legal matter amicably, only because domain name registrations were made anonymous.

“Assuming a reliable distinction can be made and verified between Legal and Natural persons, obtaining data on Legal persons would be the minimum requirement necessary to ensure transparency and enable consumers to know who they are buying from or doing business with.”

“[Differentiation provides the] Possibility to obtain data on legal persons in the course of taking actions aimed at protection of IP rights of our Clients.”

“If there was no differentiation then all Registrant data would need to be redacted in the same way. This is not required under GDPR and it would significantly hamper attempts by IP rights owners to police infringements on the internet.”

“We primarily use RDS data to investigate infringement and protect our brand/company and our customers. Clear differentiation between registration data of legitimate companies or organizations vs. data belonging to individual registrants is extremely useful in identifying and pursuing legal actions against fraud and infringement.”

Contracted Parties

The benefits of differentiation for Contracted Parties are contextual. Assuming the differentiation system is accurate and reliable, it would provide them with the ability to segment registrant clients into legal entities and natural persons. For those who do not work under the constraints of the GDPR or similar legislation, this may carry individual benefits for Contracted Parties in terms of how they manage their registration data. For those who do, differentiation could reduce the number of access requests to registration data from legitimate third-party interests; since legal person data would be available to them, these third-parties would not need to submit access requests for data not regulated by the GDPR. In any case, Contracted Parties would have to weigh these parochial benefits against the collective burden of differentiation described above.

Although from the perspective of an RDDS end-user, one respondent alluded to a potential benefit of differentiation to Contracted Parties, namely reducing the amount of data requests and complaints they receive:

“Not knowing if a registrant is a Legal or a Natural person affects the priority we assign on the filing of complaints vs. simply watching domains for release (e.g. if registered by one of our Ad Agencies). This leads to a possible added expense of creating unnecessary complaints (cost & time waste on both our end and the WIPO administration / local court ends) along with registrar transfer fees.”

Data Subjects

Natural Person Registrants

Under the GDPR, natural person data are protected. Legal person data are not (although they may contain natural person data). As noted above, in many cases Contracted Parties treat legal person data as personal data to minimize the risk of mishandling client data of violating data protection legislation. Differentiation would provide no discernable benefit to natural person registrants, as they currently have the option to allow publication of their RDDS data.⁶⁹

Legal Person Registrants

Differentiation may benefit legal person registrants who want to provide public to access their registration data by default. However, as some legal persons noted in the questionnaire, legal persons may *not* want their registration data made public by default. Differentiation by default may offer minor benefits to the former, but would not benefit the latter.

Some legal person registrants who responded to the questionnaire stated that they prefer to have their registration data available in RDDS because it provides transparency regarding domain ownership, promotes trust among users of the legal person’s Internet services, and establishes credibility. They also noted that publishing legal person RDDS data would allow third parties to contact domain owners in cases of legitimate investigations, legal disputes, technical issues, and/or DNS abuse. Responses included:

⁶⁹ ICANN.org (25 May 2018), *Temporary Specification for gTLD Registration Data*, Appendix A: Sections 2.2 – 2.4.

“Benefits of differentiation would be largely for legal entities by enabling them to have their information public. However, the risk of inadvertently breaching personal data is real and would likely outweigh the benefits.”

“Publicly publishing registrant data allows for reputational algorithms to flag my domains properly. It also provides a public record of ownership that assists with the transfer of domains and for independent audits during a merger/acquisition scenario.”

“It lends credibility to our domains and serves as one indication of legitimacy of our domains should someone question whether or not we actually operate a website associated with the domain. It also allows internal teams who may be looking for registrant data of a domain name to verify that it is company owned, avoiding the need for internal emails to verify that fact.”

“As a legal person registrant, we would like to have our registration data publicly available by default. As a legal person, whether you are a business, an association or any other type of organization, your data is already publicly available, according to the register on which the organization in question depends (i.e. trade and companies register). That is why, as a legal person registrant, we are in favour of having our registration data publicly available by default as it is the case for the offline world. In our increasingly connected world, we should definitely consider the offline world components as equivalent to the online world ones. Besides, it is important that people going to our website, are capable of knowing who the registrant is. It is a matter of Transparency and Trust. Moreover, protection of the consumer is essential in the online world where the source of the products can easily be hidden. Therefore, having the registration data publicly available would enable consumers to check the trustworthiness of a website in a more reliable way than looking at the website content. Of course, it would be even more useful if the data provided by the registrant is verified.”

“[Publishing RDDS data] provides confidence to my clients and shareholders that we are who we say we are.”

“[Publishing RDDS data] enables others to contact us so we can address technical, security or legal problems. Also gives confidence that we are running a legitimate business/operation on our domain.”

“Legal registrants who have their data visible in the RDDS outputs are viewed as more legitimate and trustworthy, where hiding behind protected data provides more of a means for ‘bad faith’ actors.”

“Since legal persons tend to be business or commercial entities there is a universal agreement among participants that customers need to be protected, and providing access to legal persons information provides security along with accountability to customers.”

“... protection of the consumer is essential in the online world where the source of the products can easily be hidden. Therefore, having the registration data publicly available would enable consumers to check the trustworthiness of a website in a more reliable way than looking at the website content. Of course, it would be even more useful if the data provided by the registrant is verified.”

However, one respondent pointed out that differentiation would provide few, if any, benefits to registrants outside the jurisdiction of the GDPR or similar data protection law:

“It is not clear what the benefits would be to registrants in the United States, since there is currently no conflict between ICANN policy with respect to WHOIS and state or federal privacy laws. Either way, U.S. registrants currently have no protection against having their information made public. The registrars seem to have chosen to redact all information, whether natural or legal and regardless of where the registrant is located, however.”

RDDS End-Users

The potential benefits of differentiation for RDDS end-users have been presented in the previous sections. In short, if RDDS data were differentiated at scale and made available in public RDDS, RDDS end-users would benefit from the increased availability of registration data.

Feasibility

In the context of this study, the **feasibility** of implementing a differentiation regime can be viewed as the difference between the sum value of risk and cost factors and the sum value of mitigatory measures and benefits associated with differentiation (this formula is applied in the model [below](#)). An ideal differentiation mechanism would be one that accurately and reliably determines whether a registrant is a legal or natural person, which would mitigate many risks to data processors associated with mishandling personal data. However, an ideal differentiation mechanism may not be **feasible** to implement if the **costs** and **risks** to one or all parties outweigh **mitigatory measures** and the **benefits** of differentiation.

The questionnaire asked Contracted Party and ccTLD respondents if they had implemented a differentiation method. Those who had received a follow-up question asking them to rank the level of effort required to implement the method. Those who had not received a similar follow-up question, but were asked to rank the level of effort they *perceived* would be required to implement a differentiation method. The results are presented in [Table 1](#) below. Note that the questionnaire was not intended to gather statistically representative samples of these populations, and thus statistical inferences should not be made. The ranking questions were intended to provide for a preliminary comparison between how parties with a differentiation method ranked the difficulty of implementing it (i.e. the “differentiators”), and those without a differentiation method ranking their *perception* of how difficult differentiation would be for them (i.e. the “non-differentiators”). The response range was provided as a standard Likert scale, with “5” indicating the highest level of difficulty, and “1” the lowest. The results show that “differentiators” generally regard differentiation as a low to medium level of effort, while the “non-differentiators” perceive it as a higher level of effort:

Table 1: Differentiation Level of Effort Rankings

Level of Effort Rankings	“Differentiators”	“Non-Differentiators”
Very low	25%	6%
Low	17%	9%
Neither high nor low	42%	12%
High	0%	15%
Very high	17%	58%

For this report, the EPDP Team requested research into “examples of industries or other organizations that have successfully differentiated between legal and natural persons.” This request was a result of Team deliberations on Charter question h3, which asked, “What mechanism is needed to ensure reliable determination of [legal or natural person] status”? The sections below provide a examples of how differentiation has been implemented both inside and outside the DNS ecosystem. They indicate that differentiation is feasible in general, but the feasibility varies depending on the jurisdictional scope and operational mission of a given party.

The following questions guided the research effort in this area:

1. Are there organizations that differentiate between legal and natural persons as it relates to GDPR? If so, what mechanisms do these organizations employ to differentiate?
2. For organizations that do not, what is their basis for not differentiating?
3. How do industries and organizations outside of the DNS ecosystem differentiate?
4. Are there other types of differentiation—i.e. not between legal and natural persons—that may be instructive to the current discussion?

Differentiation in Practice

The review of differentiation examples below, as well as many of the responses to the questionnaire, provide a number of specific suggestions that may help Contracted Parties characterize the feasibility of implementing a method to differentiate. Some may be more practical than others depending on their circumstances. They are nonetheless summarized below for reference:

1. Present clear-language explanations of registration obligations to registrants⁷⁰
2. Require registrants to periodically confirm designation as a legal or natural person⁷¹
3. Implement measures to cross-check registration information of legal persons against publicly available data (for example, a corporate registration number or organizations' contact details)⁷²
4. Apply technical mechanisms to infer whether a registrant's email addresses is that of an individual or an organization⁷³
5. Provide means to correct inaccurate designations⁷⁴
6. Provide simple choice for registrants to self-differentiate (see [below](#)), e.g.:
 - a. *INDIV* or *ORG*
 - b. "Private Individual", "Sole Proprietorship", or "Legal Person"
7. Infer status based on presence of data in the *Org* field (see [below](#))
8. Respond to RDDS queries with a NIC handle equivalent for legal person registrants, which links to additional RDDS data. Provide no such handle for natural persons.⁷⁵

DNS Industry Examples of Legal vs. Natural Person Differentiation

This study found few examples of DNS industry organizations that have implemented a differentiation regime. Not surprisingly, those that have are EU member state ccTLDs. Following the GDPR's effective date on 25 May 2018, most EU ccTLD operators continued to publish some (and sometimes all) contact data fields for domains registered by legal persons.⁷⁶ A review of the differentiation practices of 35 EU ccTLDs revealed only six that did not

⁷⁰ Bird & Bird LLP (25 January 2019), "Natural vs. Legal Memo", pp. 3-4.

⁷¹ Ibid.

⁷² Ibid.

⁷³ Ibid.

⁷⁴ Ibid.

⁷⁵ A NIC handle (Network Information Centre handle) is a unique alphanumeric character sequence representing a domain name registration in registry databases. See IETF (October 1985), "RFC 954: NICNAME/WHOIS," <https://www.ietf.org/rfc/rfc954.txt>

⁷⁶ Security and Stability Advisory Committee (14 June 2018), *SAC 101: SSAC Advisory Regarding Access to Domain Name Registration Data*, <https://www.icann.org/en/system/files/files/sac-101-en.pdf>

appear to have a differentiation regime in place.⁷⁷ EURID, the operator of the .eu TLD, publishes natural person registrants' email address and primary language, and allows for .eu registrars to provide an anonymized email option for their registrants' RDDS email field entries. For legal person registrants, it publishes the organization name, city, country, e-mail address, and primary language.⁷⁸ In some cases, per local law, ccTLD operators continued to publish certain personal data for natural person registrants. For example, Dansk Internet Forum, the ccTLD Manger for .DK, publishes the name, address, and telephone number of all registrants per Denmark's Domain Names Act of 2014.⁷⁹ Some operators address the issue of differentiation by collecting data on whether a registrant is a private individual or economic actor.⁸⁰ For example, when registering a .eu domain through the registrar Orbis, you are asked for information on the "Entity type" that is registering the domain name, such as a company, individual, or organization.⁸¹

One ccTLD operator provided a detailed response on why and how it differentiates RDDS data:

Our ccTLD has implemented a mechanism protecting personal data of domain name holders in 2006 further to exchanges with the French DPA (CNIL). Based on the recommendations of the CNIL, we set up the principle of restricted publication by default: Non-publication of personal data when registering the domain name by an individual, Free service, [sic] A registrant who can opt for publication, Disclosure of personal data under conditions: prior right or legal basis for the public authorities or upon notification of a court order ordering same. [sic] From the beginning, our registry has differentiated Legal and Natural persons to provide access to a maximum set of information regarding domain name registrants and to allow anyone to contact the registrant for any purpose. GDPR did not change our national legal framework as it still does not protect data pertaining to legal persons.

⁷⁷ For a comprehensive overview of EU ccTLDs' practices as they relate to RDDS data publication and the GDPR, see: Murphy, Kevin (25 May 2018), "How all 33 European ccTLDs are handling GDPR." *DomainIncite*, <http://domainincite.com/23053-how-all-33-european-cclds-are-handling-gdpr>

⁷⁸ EURID.eu, "WHOIS Policy," https://eurid.eu/d/205797/whois_policy_en.pdf

⁷⁹ .dk Hostmaster, "Whois and GDPR," <https://www.dk-hostmaster.dk/en/gdpr>. .DK registrants with name and address protection logged in the Danish Civil Registration System are provided anonymity in the registry's public RDDS database. See also: "Danish Act on Internet Domains," <https://www.dk-hostmaster.dk/en/danish-act-internet-domains>

⁸⁰ Kuner, Christopher, "Chapter 2: Fundamental Legal Concepts", p. 58.

⁸¹ orbis.hr, "Register Domain", <https://www.orbis.hr/portal/cart.php?a=add&domain=registerhttps://www.orbis.hr/portal/cart.php?a=confdomains>

Several respondents in the Contracted Party and ccTLD operator categories of the questionnaire described how they depend on the *Org* field to identify if a registration is that of a legal or natural person. Registrations with data present in the *Org* field are tagged as those of legal persons, and those without *Org* field data as natural person registrations. One respondent provided a representative description of the method many of these data controllers employ: “Any text entered into the organization field is treated as the Legal registrant and the first name/last name is treated as the contact at that organization.”

The EPDP Team provided a detailed recommendation regarding the use of the *Org* field as Recommendation 12 of their Phase 1 Final Report. It states :⁸²

- The Organization field will be published if that publication is acknowledged or confirmed by the registrant via a process that can be determined by each registrar. If the registered name holder does not confirm the publication, the Organization field can be redacted or the field contents deleted at the option of the registrar.
- The implementation will have a phase-in period to allow registrars the time to deal with existing registrations and develop procedures.
- In the meantime, registrars will be permitted to redact the Organization Field. A registry Operator, where they believe it feasible to do so, may publish or redact the Org Field in the RDDS output.

The EPDP Team also provided detailed implementation advice for this recommendation:⁸³

For existing registrations, the first step will be to confirm the correctness / accuracy of the existing Organization field data. For the period between the adoption of EPDP policy recommendations and the conclusion of the implementation effort set for on, or before, 29 February 2020:

1) Registrars will redact the Organization field

⁸² Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process (20 February 2019), pp. 14 – 15.

⁸³ Ibid., p. 15

2) Registrars will contact the registered name holders that have entered data in the Organization field and request review and confirmation that the data is correct.

a) If the registered name holder confirms or corrects the data will remain in the Organization field.

b) If the registrant declines, or does not respond to the query, the Registrar may redact the Organization field, or delete the field contents. If necessary, the registration will be re-assigned to the Registered Name Holder

3) If Registrar chooses to publish the Registrant Organization field, it will notify these registered name holders that of the “date certain,” the Organization field will be treated as non-personal data and be published, for those Registered Names Holders who have confirmed the data and agreed to publication.

For new registrations, beginning with the “date certain”:

1) New registrations will present some disclosure, disclaimer or confirmation when data is entered in the Organization field. Registrars are free to develop their own process (e.g., opt-in, pop-up advisory or question, locked/grayed out field).

2) If the registered name holder confirms the data and agrees to publication:

a) The data in the Organization field will be published,

b) The Organization will be listed as the Registered Name Holder.

c) The name of the registered name holder (a natural person) will be listed as the point of contact at the Registrant Organization.

After the implementation phase-in period, the ORG FIELD will no longer be REDACTED by the registrar unless registered name holder has not agreed to publication.

In contrast to the process detailed in Recommendation 12, one respondent to the questionnaire described how utilizing the Org field to differentiate was “very simple”:

The implementation of this model is very simple: the identification of a contact as an individual is based on the content of the ‘Organization’ field at the time of the registration (via EPP or Web).

- If this field is filled in by the registrant, the contact is considered a legal entity, its data being consequently published in the Whois.*
 - If the registrant does not fill in this field, the contact is considered an individual / natural person, its data not being published in the Whois.*
- If individual registrants fill in this field by mistake, they will be able to modify it as they wish.*

Several respondents criticized the use of Org field data to determine a legal or natural person designation, a method employed by some parties as evidenced by responses to the questionnaire:

There are significant costs involved in having a human attempt to determine whether a party is a Natural or a Legal person at the scale necessary to include every domain name registration, and we do not believe it is possible to distinguish this automatically. There are also significant legal risks if the determination is incorrect and data are processed inappropriately. We have determined that the costs and risks outweigh any potential benefit that could be found in differentiating by person type. For example, the presence of data in the Registrant Organization field cannot be relied upon to automatically indicate legal type.

The majority of our registrants populate the Registrant Organization field, regardless of their legal type. A customer Jane Smith might put ‘Jane Smith’, ‘none’, or ‘–’ in the Registrant Organization field, none of which can correctly be assumed to mean that she is actually an Organization. Similarly, she might put ‘Jane Smith Co.’ without actually being a corporation, or indicate that she is a Legal person rather than Natural person if the option is presented, not understanding the distinction and the fact that this would allow her personal privacy rights to be infringed.

“It is unfeasible to do so since registrants have been using the ‘Organization’ field for anything they felt like. We found the contents of this field to be generally unreliable when trying to assess what class a registrant belongs to. While in some cases, it may be apparent, in others it is not.”

Another instructive example of differentiation in the DNS industry comes from RIPE-NCC, a Regional Internet Registry (RIR) serving a broad swathe of countries in Europe, Asia, and the Middle East, that publishes a database of Internet numbering resources and contact details of those responsible for them. RIPE-NCC states: “[f]acilitating coordination between network operators (network problem resolution, outage notification etc.)...is the one [purpose] that justifies the publication of personal data in the RIPE-NCC Database”, and that “it is clear that the processing of personal data referring to a resource holder is necessary for the performance of the registry function, which is carried out in the legitimate interest of the RIPE community and the smooth operation of the Internet globally (and is therefore in accordance with Article 6.1.f of the GDPR).”⁸⁴ RIPE-NCC publishes all contact details regardless of whether the data subject is a legal or natural person, noting that the contacts “are usually the technical and administrative employees of the natural or legal persons that hold the resources,” and contain the names of the resource holders and/or a designated representative of that resource holder, as well their “(business) email addresses, (business) phone and fax numbers, and (business) postal addresses.”⁸⁵ RIPE-NCC concludes: “our assessment indicates that current operations are in line with the legislation.”⁸⁶

The examples above illustrate that differentiation is feasible for EU ccTLDs, and that in some cases—e.g. RIPE-NCC—publishing natural person data is may not necessarily violate the GDPR if a data processor has a defensible legal purpose for doing so. However, the determination as to whether such a purpose is legally defensible remains with lawyers representing data controllers, processors, DPAs, and courts. In sum, local law and the specific purposes behind data processing influence how many parties handle personal data.

Non-DNS Industry Examples of Legal vs. Natural Person Differentiation

A look outside of DNS industry players is only partially instructive due to the unique nature of domain name registration data and the types of data processing that are required. Generally, data-processing organizations impacted by the GDPR outside the DNS ecosystem do not have contractual or

⁸⁴ RIPE-NCC refers to the following language from Article 6.1.f: “Processing shall be lawful only if and to the extent that at least one of the following applies: ... (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...”. See: RIPE Labs (6 March 2018), “How We’re Implementing the GDPR: Legal Grounds for Lawful Personal Data Processing and the RIPE Database”, <https://labs.ripe.net/Members/Athina/gdpr-legal-grounds-for-lawful-personal-data-processing-and-the-ripe-database>

⁸⁵ RIPE Labs (1 February 2018), “How We’re Implementing the GDPR: The RIPE Database”, <https://labs.ripe.net/Members/Athina/how-we-re-implementing-the-gdpr-the-ripe-database>

⁸⁶ Ibid.

policy obligations derived from a global multi-stakeholder process. They adhere to the general principles of the GDPR to the extent relevant for their data-processing activities. As it considers the question of differentiation, a Contracted Party is faced with the risk of potentially disclosing personal data in RDDS.⁸⁷ While all organizations affected by the GDPR must consider issues of consent, accuracy, and how to identify personal data, non-DNS industry organizations typically do not have an added layer of disclosure constraints and obligations determined by an outside process, which makes the relationship between how these organizations differentiate between legal and natural persons (or in other ways) less analogous to how organizations would differentiate in the ICANN ecosystem.

The Phone Book

Prior to the GDPR's effective date on 25 May 2018, ICANN org engaged with the Hamilton Law Firm to address a number of questions on the impact of the GDPR on RDDS. One asked: "When and how does the GDPR apply to personal data processing related to the domain name system functions? As a comparison, are telephone books permissible in the EU? Would sending them outside the EU be a violation of the GDPR?"⁸⁸ While Hamilton did not address this question in the context of telephone directories, it brings up what may be the most relevant example of differentiation outside the DNS industry. The "phone book" provides a directory of all listed phone numbers in a given locale. Many parallels can be drawn between how individuals and businesses were listed in phone books and the issue facing the EPDP team as it relates to differentiation of legal and natural persons. For much of the 20th century, the phone book was the go-to for contact information of both individuals and businesses.

Up until 2010, regulators in the United States required telecommunications companies to publish directories of the phone numbers (landlines) of local subscribers. These listings were known as the "white pages," as they were printed on white paper. The white pages differed from the "yellow pages" which included only business listings paid for by the business wanting to be listed, which were printed on yellow paper.

⁸⁷ Bird & Bird LLP (25 January 2019), "Natural vs. Legal Memo", p. 2.

⁸⁸ Hamilton Advocatbyra (16 October 2017), "Memorandum: gTLD Registration Directory Services and the GDPR - Part 1," <https://www.icann.org/en/system/files/files/gdpr-memorandum-part1-16oct17-en.pdf>, Appendix 1.

While the yellow pages included only the numbers of businesses, the white pages could include both residential and business listings, or even government listings, depending on the area. Individuals were included in the listing at no cost when they signed up for a landline, but telephone companies often charged advertising fees to be listed in the business white pages. Individuals were therefore differentiated from businesses when they signed up for the landline through their service provider; a business would have to declare itself as a business in order to be listed in the business white pages.

All residential subscribers were automatically listed, but individuals not wanting to have their information listed usually had two options, often for a monthly fee:

- **Non-listed (semi-private)**: information is not published in the white pages but is available through directory assistance.
- **Unpublished (private)**: information is neither published in the white pages nor available via directory assistance.

However, due to the cost of having a phone number made private, some individuals would simply sign up with fake names to mask their identity in the white pages.

To be included in the yellow pages, businesses needed to pay, much like buying an ad space. Indeed, the yellow pages were for much of the 20th century part of a hugely successful advertising industry: “Since its advent in the late 1800s, publishers of the yellow pages have operated a simple business model: A sales force charges local businesses for advertising, and the publisher ships a booklet of these advertisements—alongside a directory of businesses’ phone numbers—to customers’ doorsteps.” The yellow pages represented the primary means by which consumers could get in touch with businesses. A business that did not pay to list itself in the yellow pages would face significant disadvantages in terms of marketing to its customer base compared to those that did.

While the white pages served as a listing for all registered phone numbers, the yellow pages provided an avenue to promote and advertise a business with larger and more detailed graphics. The holder of the business phone number could pay a base fee for a simple listing, or pay extra for more space

and graphics such as company logos. Such a model may be instructive in terms of the current discussion on differentiation. If it were to be applied to RDDS data, businesses—i.e. legal person registrants—would have to proactively “opt-in” in order to have their business listed. While a fee to be listed, or additional fees for more features, may not apply to RDDS, legal persons registrants could be presented with an option to be listed in a “yellow pages” of the RDDS. If legal registrants did not opt-in to the “yellow pages,” then their information would not be made public. Natural person data would be left unpublished along with those of any other registrants who prefer to keep their data private.

The white pages provides a closer analogue to RDDS. Processing white page data resembled how the RDDS system worked in a pre-GDPR world: data was published by default for both legal and natural persons, but holders of a phone number were provided with an option to keep their data private. This resembles the current practice among many registrants to pay an additional fee for a privacy/proxy service to mask their RDDS data. Accuracy issues were also similar. Some individuals, for various reasons, chose to mask their true identity to prevent having their information published.

As a result of the GDPR, personal data that could theoretically have been included in the “white pages” of RDDS are now redacted for the most part. However, the current policy allowing all registrants to opt-in to data publication in RDDS resembles those governing the processing of data for the white pages: consent is obtained by default as registrants must opt-in to have their registration data listed publicly. Unlike business listings in phone books, registrants do not have to pay to be “listed” in RDDS; it is a fee-free option mandated in the *Interim Policy*.⁸⁹ While many personal data are redacted in RDDS for those registrations subject to the GDPR or similar legislation, registrants may also pay a privacy/proxy service to mask their registration data. Regardless of the fee structure—or lack thereof—when registrants “opt in” to data publication in RDDS, they signal they understand and have been informed of the implications. The “opt in” policy thus works to reduce a number of risks associated with inadvertently publishing personal information since registrants must specifically indicate if they want their data available in public RDDS.

⁸⁹ ICANN.org (25 May 2018), *Temporary Specification for gTLD Registration Data*, Appendix A: Sections 2.2 – 2.4.

Banking

A study conducted by Deloitte in 2019, one year after the GDPR went into effect, found that “in general, financial services companies have more easily taken [the regulation] in their stride than companies in other sectors. This is because they have a long history of complying with strict privacy and data protection rules set by financial regulators.”⁹⁰ A requirement for public disclosure of client data as it faces Contracted Parties in terms of the differentiation does not exist for banks due to the strict regulations surrounding financial services.

Financial institutions differentiate between personal and business accounts. In most cases, the data collected for a personal compared to a business account differs. A user is typically required to file a separate application and meet separate requirements for a business account. For example, when opening a Chase business account, an applicant is required to provide specific information about the business--regardless of whether that business is a sole proprietorship or a large corporation--such as a tax ID, a Doing Business As (DBA) certificate or other documentation providing evidence of incorporation.⁹¹ This echoes suggestions made by Bird & Bird in their advice on how to differentiate in the gTLD space: “To separate corporate entities from natural persons, registrants could be required to provide a corporate registration ID number when registering on behalf of a company. This would allow the registrar to detect internal inconsistencies, such as if a registrant identifies as a corporate entity but is unable to provide a valid ID number.”⁹² A key difference between the banking and DNS industries as in relation to differentiation is that banks face no obligation to disclose data based solely on whether it is an account “personal” or “business” account” (this is likely illegal in most jurisdictions).

Travel Loyalty Programs

Another similar case is airline travel frequent flyer/loyalty programs, such as frequent flyer or car rental programs. Many airlines offer both personal frequent flyer accounts as well as business accounts. For example, both American and Delta airlines offer programs to allow both the individual

⁹⁰ Deloitte (2019), “After the dust settles: How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on”, <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-the-impact-of-gdpr-on-the-financial-services.pdf>.

⁹¹ chase.com, “Choose what’s right for your business,” <https://www.chase.com/business>

⁹² Bird & Bird LLP (25 January 2019), “Natural vs. Legal Memo”, p. 4.

employee and the company they work for to earn miles or points for travel; the points are accumulated differently and are spent on different perks.⁹³ As with a business bank account, the user applies via a separate application and website for a business frequent flyer account, and is required to provide additional information regarding the business, such as a tax ID. Enterprise, a rental car company, offers “solutions for business” and has a car rental program for small and medium-sized businesses. Companies apply to join the program and can receive special corporate deals and promotions.⁹⁴ The differentiation between a legal and natural person is again inherent to the natural separation of the two types of accounts. As with the business bank account example, this type of differentiation is in line with suggestions from Bird & Bird, though not entirely analogous to the situation facing Contracted Parties. Travel companies offering these programs face no obligation to disclose clients’ data based on whether their clients are natural or legal persons.

Direct Marketing

Direct marketing is one business activity that has been heavily affected by the GDPR. The GDPR itself does not define “direct marketing,” but the Data Protection Act from the United Kingdom offers the following definition: “‘direct marketing’ means the communication (by whatever means) of advertising or marketing material which is directed to particular individuals.”⁹⁵ Direct marketing is often divided into Business-to-Customer (B2C) and Business-to-Business (B2B).⁹⁶ The UK Independent Commissioners Office (ICO) states, in response to the question of whether the GDPR affects B2B direct marketing, that “[t]he GDPR applies wherever you are processing ‘personal data’. This means if you can identify an individual either directly or indirectly, the GDPR will apply - even if they [sic] are acting in a professional capacity.”⁹⁷ For direct marketing professionals working under the GDPR,

⁹³ [businessextra.com](https://www.businessextra.com/home.htm), “Real value for companies with air travel,” <https://www.businessextra.com/home.htm> and [delta.com](https://skybonus.delta.com/content/skybonus/corporate/us/en/home.html), “The No-Cost, Simple Way to Maximize Your Company’s Travel Budget,” <https://skybonus.delta.com/content/skybonus/corporate/us/en/home.html>.

⁹⁴ [enterprise.com](https://www.enterprise.com/en/business-car-rental.html?icid=header.business.solutions_-_business.rental), “Car Rental Program for Small and Medium Sized Businesses,” https://www.enterprise.com/en/business-car-rental.html?icid=header.business.solutions_-_business.rental

⁹⁵ [legislation.gov.uk](http://www.legislation.gov.uk/ukpga/2018/12/section/122/enacted), Data Protection Act 2018, <http://www.legislation.gov.uk/ukpga/2018/12/section/122/enacted>

⁹⁶ Rėklaitis, Kešutis & Pilelienė, Lina. (2019). Principle Differences between B2B and B2C Marketing Communication Processes. Management of Organizations: Systematic Research. 81. 73-86. doi: 10.1515/mosr-2019-0005.

⁹⁷ UK ICO, “The rules around business to business marketing, the GDPR and PECR”, <https://ico.org.uk/for-organisations/in-your-sector/marketing/the-rules-around-business-to-business-marketing-the-gdpr-and-pecr/>

the question emerges as to how companies could differentiate between personal and business contact information to conduct their marketing campaigns. One company, Sonovate, discusses their process as follows:

Initially, you can segment your existing mailing lists between what you recognise as personal data versus business data. For example, you can add all the @hotmail, @gmail or @btinternet type email addresses into a B2C list and all business name ones into your B2B list. Then when you ask for people to fill in their details, on your website for instance, you could ask them for a few more bits of information to gauge whether you're dealing with a business or an individual. You could ask for their company name and maybe how many employees are at the company, so you can estimate the size of the company too. It will not tell you for sure, but you should be able to get a good idea from asking for this information.⁹⁸

Sonovate describes a risk mitigation strategy similar to those employed by some ICANN Contracted Parties, that is to “treat everyone as an individual and ask for active consent when they give you their details.”⁹⁹ Marketing Eye, a marketing consultancy, describes a similar strategy, stating: “one sure-fire way of staying GDPR compliant is to treat your B2B and B2C contacts the same.”¹⁰⁰

Everstring, an “AI-assisted SaaS for B2B,” states in its privacy policy that “[i]f EverString obtains Business Contact Information regarding an individual that EverString has reason to believe is based in the European Union, EverString will preemptively anonymize and aggregate such information.”¹⁰¹ The company states in a video on “Verified Contacts” that “your [contact] list will only contain contacts from within the US due to GDPR constraints.”¹⁰²

⁹⁸ Sonovate, “Key differences between B2B and B2C when it comes to GDPR”, <https://www.sonovate.com/blog/key-differences-b2b-b2c-gdpr/>

⁹⁹ Ibid.

¹⁰⁰ The Marketing Eye (19 December 2017), “GDPR: B2B vs B2C – can you still email your database?”, <https://www.themarketingeye.com/blog/gdpr-b2b-vs-b2c-can-you-still-email-your-database/>

¹⁰¹ everstring.com, “Privacy Policy”, <https://www.everstring.com/privacy-policy/>

¹⁰² everstring.com, “Contacts - EverString Overview Demo,” <https://vimeo.com/357684590>

The UK ICO offers guidance on employing “legitimate interest” to justify processing personal data resulting B2C and B2B data sharing: “You can consider using legitimate interests as your lawful basis for such processing. However you need to identify your specific interest underlying the processing and ensure that the processing is actually necessary for that purpose.”¹⁰³ This strategy aligns with the strategy used by RIPE discussed in the previous section: a legitimate purpose for processing personal data may provide a basis for compliance with the requirements of the GDPR

Social Media and Age-related Content

A number of prominent social media companies differentiate online according to user age, for activities such as creating accounts, accessing content, and purchasing goods. For example, Facebook, Snapchat, and TikTok require users to be at least 13 years old. Youtube requires account holders to be at least 18 years old, but younger users can obtain an account with parental consent.¹⁰⁴ For these companies, differentiation is straightforward: simply collect the user’s birth date upon account creation.

In the United States, drinking alcohol is illegal for anyone under 21 years old. Alcohol producers and retailers in the US often differentiate according to age, allowing only those who indicate they are 21 or older to view their websites. Although there is no legal requirement for “age gates,” many alcohol-related websites contain one.¹⁰⁵ The efficacy of these age gates is debatable, and raises accuracy issues similar to those present in RDDS. Underage users can simply enter a “21 or older” birth date to view the content. However, in some cases, companies will attempt to verify the age of a user. Google, Youtube’s parent company, will verify a user’s age using a valid credit card or copy of a government issued ID in cases when an account is disabled due to a possible violation of the age restriction.¹⁰⁶

¹⁰³ UK ICO, “When can we rely on legitimate interests?”, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/>

¹⁰⁴ Independent (31 January 2019), “Social Media Being Used By Growing Number Of Children Under 11 Despite Age Limits”, <https://www.independent.co.uk/life-style/children-social-media-use-age-limit-facebook-instagram-profiles-a8756096.html>

¹⁰⁵ Huffington Post (21 September 2017), “The Surprising Truth About Why Alcohol Websites Make You Enter Your Age”, https://www.huffpost.com/entry/liquor-website-age-verification_n_59c3b549e4b06f93538cdd18

¹⁰⁶ google.com, “Frequently Asked Questions about Google Accounts & Age Requirements”, <https://support.google.com/accounts/answer/1333913>

In the United States, the Children's Online Privacy Protection Act (COPPA) “specifically protects the privacy of children under the age of 13 by requesting parental consent for the collection or use of any personal information of the users”; violators of the regulation can incur fines up to \$42,530.¹⁰⁷ The United States Federal Trade Commission (FTC) offers a six-step COPPA compliance plan for companies impacted by the regulation.¹⁰⁸ The plan carries many elements similar to the GDPR’s in terms of consent, with the primary difference being that a child’s parent must provide it. In the plan, the FTC recommends that online alcohol retailers pursue “third-party age verification before consumers can purchase alcohol online,”¹⁰⁹ which is similar to Bird & Bird’s suggestion that Contracted Parties could employ a third-party to verify the accuracy of a legal or natural person designation in RDDS.¹¹⁰ However, with regard to the purchase of alcohol (or even viewing of alcohol-related content), the risk of providing a false date of birth falls on the website visitor (the “data subject” in this case): if caught, he/she could be prosecuted under the US Computer Fraud and Abuse Act (CFAA).¹¹¹ In contrast, the risk and potential cost of an inaccurate legal or natural person designation falls almost entirely on data controllers and processors under the GDPR.

¹⁰⁷ Federal Trade Commission (22 November 2019), “YouTube channel owners: Is your content directed to children?”, <https://www.ftc.gov/news-events/blogs/business-blog/2019/11/youtube-channel-owners-your-content-directed-children>

¹⁰⁸ Federal Trade Commission, “Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business”, <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>

¹⁰⁹ *Ibid.*

¹¹⁰ Bird & Bird LLP (25 January 2019), “Natural vs. Legal Memo”, p. 4.

¹¹¹ United States Justice Department (14 January 2015), *Prosecuting Computer Crimes*, <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>

Differentiation Scenario Model

The model below is built on the research presented above, and serves as a framework for the EPDP Team to compare the *status quo* against a hypothetical policy to differentiate. The aim is to provide a structure for the Team to assess the **feasibility** of differentiation in terms of **cost**, **risk**, **mitigation**, and **benefits** to Contracted Parties, registrants, and RDDS end-users.

Important Notes and Caveats

- The ICANN Board's adoption of the *Temp Spec* spurred the ICANN Community to start the EPDP in order to develop a registration data policy that complies with the GDPR. Thus, the GDPR represents a key condition of the model. The legal environment is controlled to assess the potential impact of the factors noted above on the feasibility of implementing a differentiation regime under the GDPR and similar legislation.
- A model is by definition an abstraction of reality. The one presented here is premised on asserting "stark and simplifying propositions" distilled from the research presented above in order to reduce non-essential complexities.¹¹² It serves as an analytical rather than prescriptive tool.
- Quantitative data is not available at the scale needed to make statistical inferences. The model is based solely on qualitative research findings.
- The model assumes a hypothetical causal relationship between a decision to differentiate and the emergence of costs, risks, mitigation measures, and benefits. This relationship cannot be rigorously tested given time constraints and the qualitative nature of the research questions.

¹¹² Mancur Olson, a prominent political scientist who wrote extensively on the collective action problem, described his research approach as "looking for the areas where there can be a breakthrough—for areas where strong claims are in order. Thus I think it is a good research strategy to search for stark and simplifying propositions." Oates, Wallace, Joe Oppenheimer, and Thomas C. Schelling. "In Memoriam: Remembering Mancur Olson." *Southern Economic Journal* 66, no. 3 (2000): 793-800. www.jstor.org/stable/1061440

- **Cost, risk, mitigation,** and **benefits** are operationalized as variables in the model and weighed against each other to calculate a relative feasibility value. An absolute quantitative value cannot be assigned to these variables. Instead, they carry *relative* values based on logical inference as to whether a given factor impacts a party negatively, positively, or has no effect (or an effect cannot be determined).
- Any values presented herein are for informational and discussion purposes only. They do not represent definitive statements on the actual value of a given variable, but serve as a starting point for the EPDP Team and ICANN Community to discuss the relative merits of differentiation. The EPDP Team and ICANN Community are expected and encouraged to assess these values in their deliberations. In short, the model is a tool for the EPDP Team and ICANN Community to use during their assessment of differentiation.
- The model is built on assigning basic *positive, negative, or null* values to each variable as they relate to a given party. The actual value of each variable to a party may differ in intensity, however. Some variables may have a relatively higher or lower impact than others for a given party. In other words, ***the degree of impact is not accounted for in the model.***

Model Key

Natural Person DNRD: *personal* DNRD associated with an individual

Legal Person DNRD: *non-personal* DNRD associated with an organization*

* Legal person DNRD may contain natural person data.

Process: to collect, transfer, display and/or redact DNRD per applicable data protection law and current ICANN policy

RDDS: Registration Data Directory Services

Contracted Parties: ICANN-accredited domain name registries and registrars

Data Subjects: Domain name registrants

End-Users: Users of Registration Data Directory Services (e.g. law enforcement, legal interests, researchers)

Red text/shading indicate **risk** and **cost** factors that **decrease feasibility**.

Green text/shading indicate **mitigation** and **benefit** factors that **increase feasibility**.

Orange text/shading indicates **parity or an undefined balance** between **risk, cost, mitigation** and **benefit** factors.

Problem Synopsis

Differentiation between **legal** and **natural persons** in **RDDS** allows for the **domain name registration data (DNRD)** of legal persons to be treated as **non-personal data**, which could thus be published in RDDS without violating data protection laws such as the GDPR. ICANN **Contracted Parties**—domain name registries and registrars—would face uncertain **risks** and **costs** in terms of implementing a program to differentiate DNRD. However, differentiation may be **feasible** if the measures to mitigate these **risks** and **costs** are economical and reliable, and if the of **benefits** of differentiation make the effort worth the potential risks and costs. The objective of the model is to provide a method to weigh the **cost** and **risk** of differentiation to Contracted Parties, registrants, and RDDS end-users against the impact of **mitigation** measures and the **benefits** of differentiation, with an aim to assess the **feasibility** of differentiation as it relates to each party and the RDDS ecosystem as a whole.

Variables and Measurement

Although the relationships between the variables presented below cannot be rigorously tested, it is nonetheless instructive to frame the problem in terms of a hypothetical relationship between them. This helps to separate the complexity of differentiation into component parts, which allows for a deeper analysis of the potential effects of differentiation. The following factors have been identified as the primary variables relevant to this study, characterized in terms of their variable type:¹¹³

“Legal Environment”

- **Control Variable:** a constant and unchanging standard used to make comparisons.
- The “legal environment” is controlled to assess the relationship between the variables under the conditions of the GDPR. In other words, the model is relevant only under the conditions of the GDPR or similar data protection legislation.

¹¹³ Van Evera, Stephen (1997), *Guide to Methods for Students of Political Science*, Cornell University Press.

“Differentiation” (*D*)

- Independent Variable: The causal variable(s) hypothesized to have an effect on the dependent variable (i.e. the outcome).
- Differentiation is conceived of as an independent variable because in the model, it “causes” **Risks** and **Costs**
- Differentiation is treated as a “dummy” variable, that is to differentiate (1), or not (0)

“Mitigation” (*M*)

- Intervening Variable: a variable contributing to the effect of the independent variable on the dependent.
- **Mitigation** efforts “intervene” in the hypothetical process presented in the model. They may lessen the **Risks** and **Costs** of differentiation, and thus may impact the **feasibility** of differentiation.

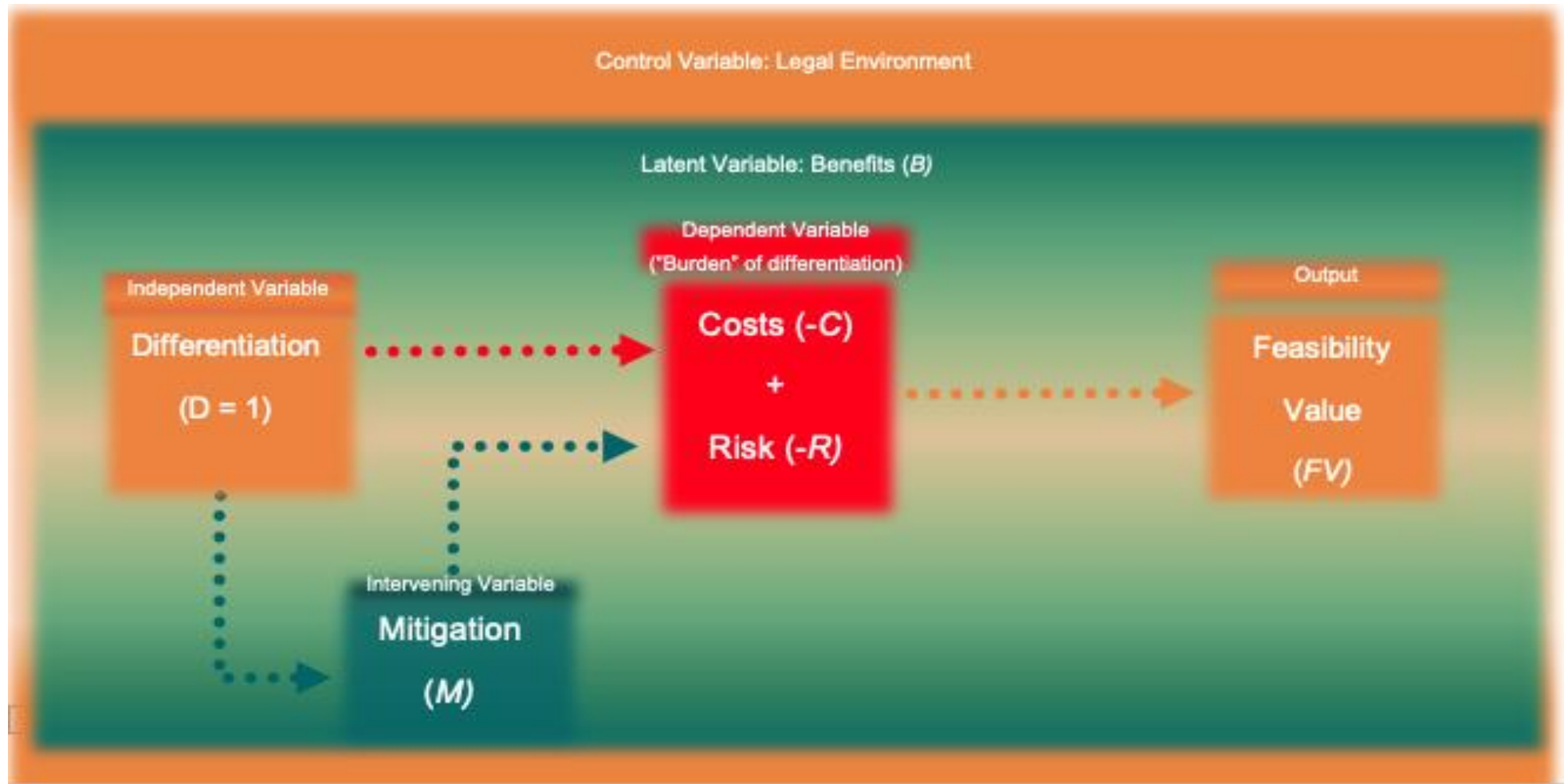
“Benefits” (*B*)

- Latent Variable: a variable that cannot be directly observed or measured, but is inferred.
- **The benefits** of differentiation are for the most part collective, and thus dispersed across a large population. **Benefits** cannot be directly measured, yet some systemic benefit is assumed.

“Burden” [**Cost** (-*C*) + **Risk** (-*R*)]

- Dependent Variable: The outcome variable resulting from the effects of the independent variable and any others that precede it in a hypothesized causal chain.
- **Risks** and **Costs** are conceived of as a singular dependent variable—the “Burden” of differentiation—that are “caused by” differentiation. They result from a positive (+1) decision to differentiate on the part of a Contracted Party. However, **mitigation measures** and **benefits** associated with differentiation may reduce the weight of the Burden.

These variables are compared to calculate a relative **Feasibility Value (FV)** for each party. Graphic X provides a “hypothesis map” illustrating the proposed relationship between them should a Contracted Party decide to differentiate ($D = 1$):



The following hypothesis statements are derived from the hypothetical assertions presented above, and serve as the basis for scoring the impact of differentiation on Contracted Parties, registrants, and RDDS end-users:

Hypothesis 0 (H0, Null)

The **costs** and **risks** of differentiation are **at parity** with **mitigation** efforts and the **benefits**. This equates to an “**infeasible**” effort.

Hypothesis 1 (H1)

Differentiation imposes **costs** and/or **risks** that outweigh **mitigation** efforts and **benefits**. This equates to an “**infeasible**” effort.

Hypothesis 2 (H2)

The **benefits** of differentiation combined with **mitigation** efforts outweigh the **costs** and **risks**. This equates to a “**feasible**” effort.

These hypotheses are encapsulated in the following formula, which is applied in the remaining sections of this model:

$$[\text{Risk } (-R) + \text{Cost } (-C)] + [\text{Mitigation } (M) + \text{Benefits } (B)] = \text{Feasibility Value } (FV)$$

Feasibility values are calculated below using this formula. The calculation method is based on logical inference from the research presented above as to whether a variable has a positive, negative, or null effect on a given party:

A variable that has a negative effect on a party is assigned a score of – 1 and **shaded in red**.

A variable that has a null or undefined effect on a party is assigned a score of 0 and **shaded in orange**.

A variable that has a positive effect on a given party is assigned a score of 1 and **shaded in green**.

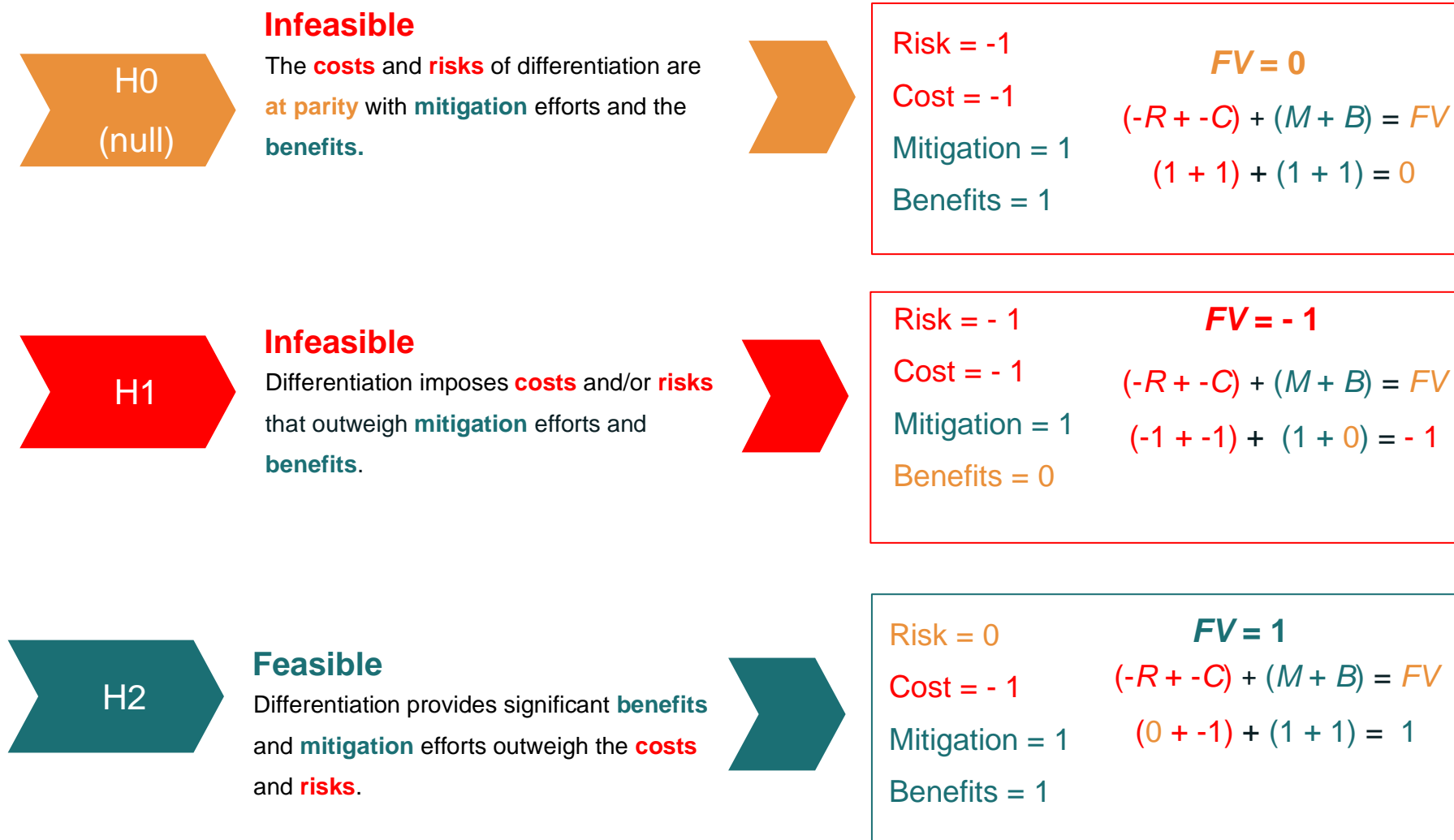
Feasibility Assessment Heat Map Key

The results provide values ranging from -4 to +4. The factors constituting the risks, costs, benefits, and mitigation measures listed in the heat maps are derived from the research presented to this point. The factors have been reduced to succinct summary terms or phrases, and have been hyperlinked to the relevant pages in the report to illustrate the basis for a factor being listed in a given category and/or assigned to a given party. The schema for the output is as follows:

$$[\text{Risk } (-R) + \text{Cost } (-C)] + [\text{Mitigation } (M) + \text{Benefits } (B)] = \text{Feasibility Value } (FV)$$

	Risks	Costs	Mitigation	Benefits	FV
Contracted Parties	[Risk factors listed here]	[Cost factors listed here]	[Mitigation factors listed here]	[Benefit factors listed here.]	(-4 thru +4)
Natural Person Registrants	[Risk factors listed here]	[Cost factors listed here]	[Green shaded boxes assigned +1 feasibility point]	[Benefit factors listed here.]	(-4 thru +4)
Legal Person Registrants	[Risk factors listed here]	[Cost factors listed here]	[Mitigation factors listed here]	[Red shaded boxes assigned -1 feasibility point]	(-4 thru +4)
RDDS End-Users	[Risk factors listed here]	[Orange shaded boxes assigned 0 feasibility points]	[Mitigation factors listed here]	[Benefit factors listed here.]	-(4 thru +4)

The graphic below provides examples of how results are calculated. Null results are characterized as “infeasible” based on the general rule that deviation from a *status quo* imposes costs. 0 net benefit would thus not incentivize differentiation on the part of a given party.

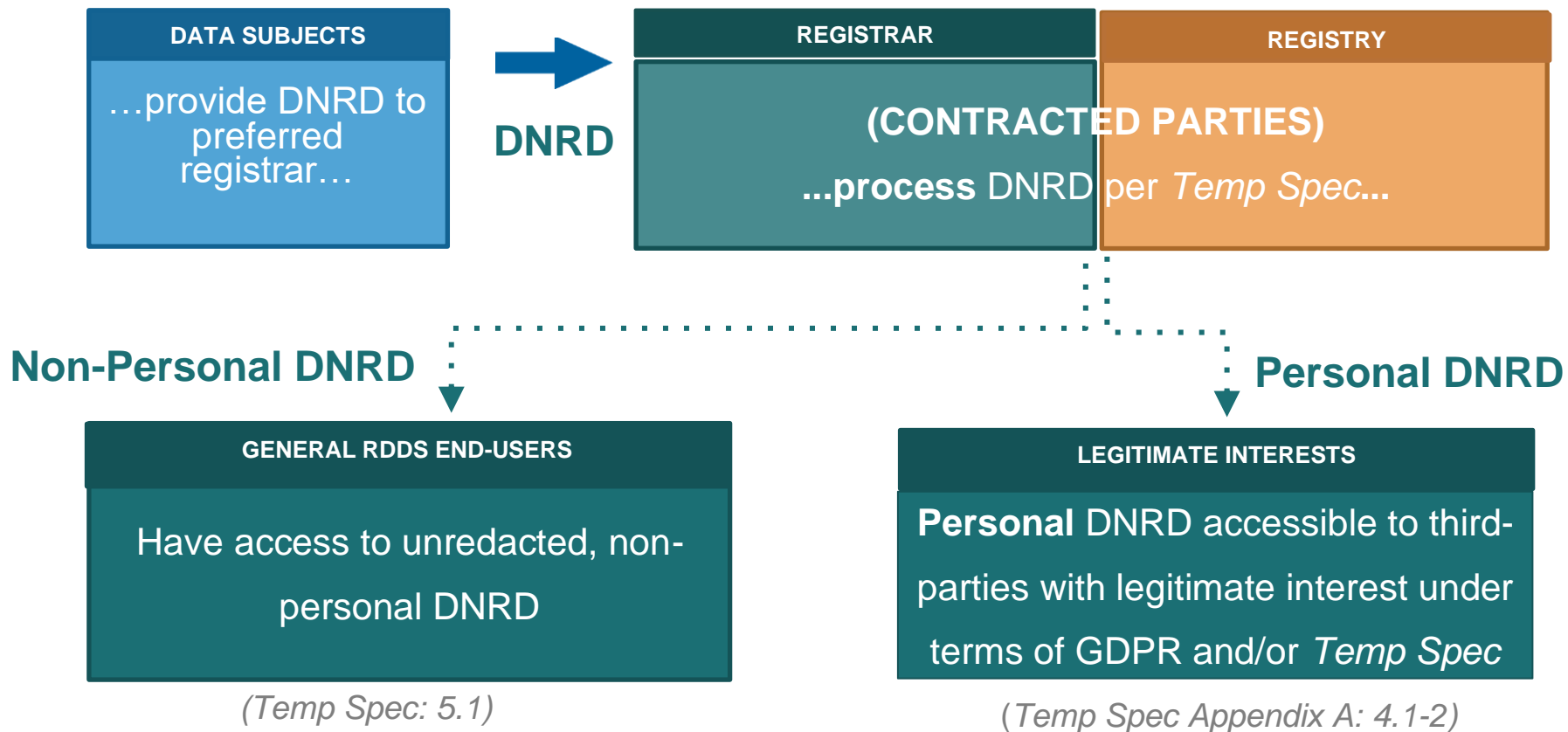


Scenario 0: No Differentiation

Scenario 0: “No Differentiation” Process Map

The basic procedure of the *Interim Registration Data Policy* is represented below in reduced form *without* differentiation as an option. A data subject provides DNRD to a Contracted Party who treats all RDDS data as if it contains personal data, i.e. redacts personal data fields per the requirements of the *Temp Spec* (see Section 7.2 and Appendix A: 2.2 – 2.4). Those data are available to users that have a legitimate interest that is not outweighed by the fundamental rights and freedoms of the registrant. In the model, any DNRD that may be published in RDDS are referred to in the model as “non-personal” DNRD.

(Temp Spec: Appendix C)











Scenario 0: “No Differentiation” Feasibility Assessment Heat Map

$$[\text{Risk } (-R) + \text{Cost } (-C)] + [\text{Mitigation } (M) + \text{Benefits } (B)] = \text{Feasibility Value } (FV)$$

	Risks	Costs	Mitigation	Benefits	FV
Contracted Parties	N/A	N/A	N/A	N/A	0
Natural Person Registrants	N/A	N/A	May consent to publish RDDS data (p. 28)	Privacy (p. 23)	2
Legal Person Registrants	Credibility Authenticity Reachability (p. 24)	Credibility Authenticity Reachability (p. 24)	May consent to publish RDDS data (p. 28)	Privacy (e.g. personal data associated with legal person registrants) (p. 2424)	0
RDDS End-Users	Fewer RDDS data reduces effectiveness of work (p. 24)	IP infringement Less effective law enforcement online Less comprehensive research Commercial revenues decreased (p. 24)	N/A	N/A	-2

Scenario 0: “No Differentiation” Feasibility Value by Party

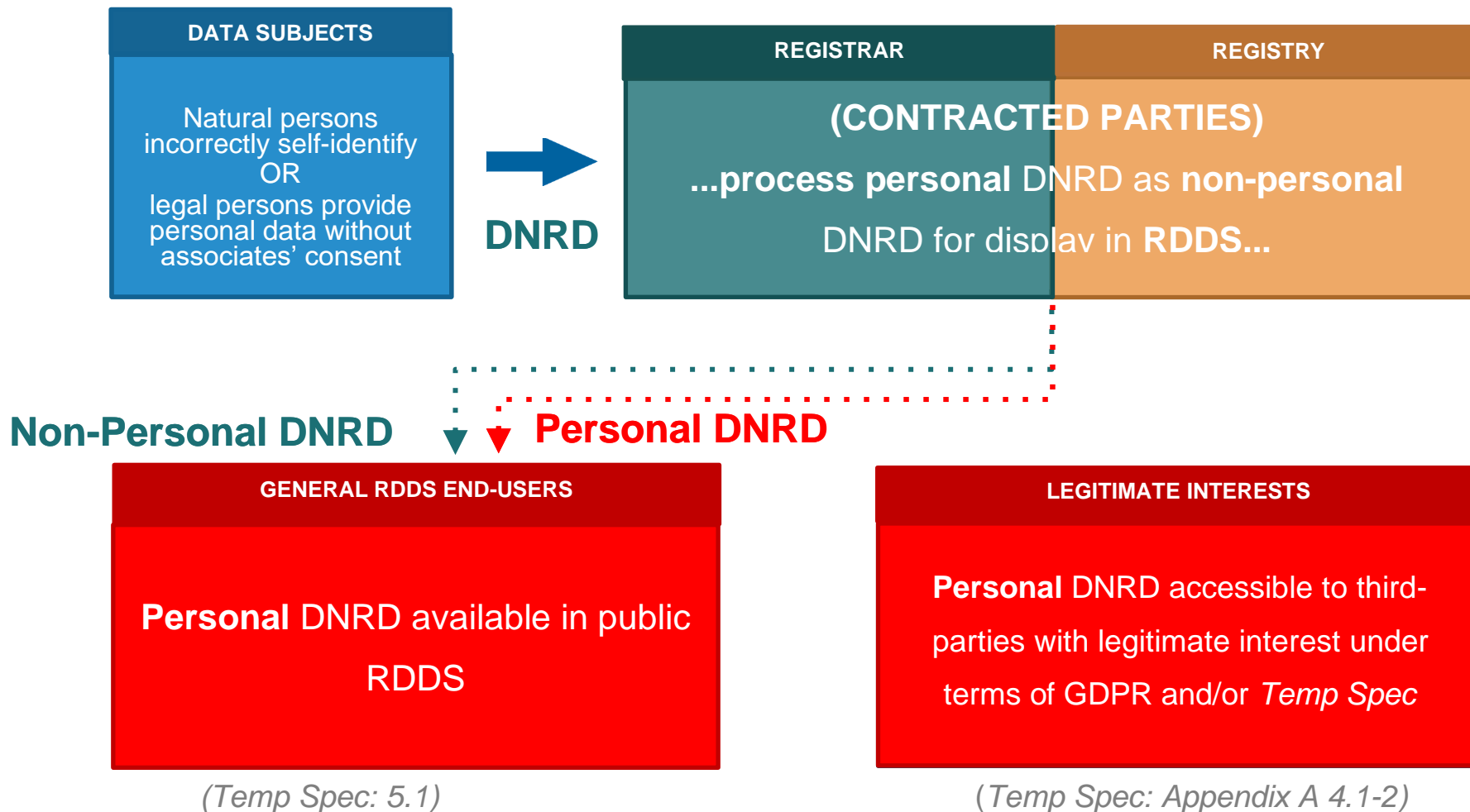
	Contracted Parties		<p>Risk = 0</p> <p>Cost = 0</p> <p>Mitigation = 0</p> <p>Benefits = 0</p>	<p>$FV = 0$</p> <p>$(-R + -C) + (M + B) = FV$</p> <p>$(0 + 0) + (0 + 0) = 0$</p>
	Natural Person Registrants		<p>Risk = 0</p> <p>Cost = 0</p> <p>Mitigation = 1</p> <p>Benefits = 1</p>	<p>$FV = 2$</p> <p>$(-R + -C) + (M + B) = FV$</p> <p>$(0 + 0) + (1 + 1) = 2$</p>
	Legal Person Registrants		<p>Risk = 0</p> <p>Cost = 0</p> <p>Mitigation = 1</p> <p>Benefits = 0</p>	<p>$FV = 0$</p> <p>$(-R + -C) + (M + B) = FV$</p> <p>$(-1 + -1) + (1 + 1) = 0$</p>
	RDDS End-Users		<p>Risk = -1</p> <p>Cost = -1</p> <p>Mitigation = 0</p> <p>Benefits = 0</p>	<p>$FV = -2$</p> <p>$(-R + -C) + (M + B) = FV$</p> <p>$(-1 + -1) + (0 + 0) = -2$</p>

Scenario 1: Registrant Self-Identification

Scenario 1: Registrant Self-Identification Problem Map

The following process map illustrates a scenario in which a registrant provides personal data, i.e. as a natural person registrant OR as a legal person registrant on behalf of associates without their consent (e.g. the *Tech* and/or *Admin* contacts of a domain name registration):

(Temp Spec: Appendix C)



Scenario 1 (Registrant Self-Identification): Feasibility Assessment Heat Map

$$[\text{Risk } (-R) + \text{Cost } (-C)] + [\text{Mitigation } (M) + \text{Benefits } (B)] = \text{Feasibility Value } (FV)$$

	Risks	Costs	Mitigation	Benefits	FV
Contracted Parties	Natural person registrant mis-identifies as a legal person; personal RDDS data flagged for availability in public RDDS (p. 20)	Liability depending on severity of violation (p. 12)	Verify registrant designation [neutral value assigned as verification is a cost as well as mitigation measure] (p. 31)	N/A compared to <i>Scenario 0</i>	-2
Natural Person Registrants	May mis-identify as legal persons; personal RDDS data flagged for availability in public RDDS (p. 20)	Privacy (p. 23)	N/A	N/A	-2
Legal Person Registrants	Identifies as a legal person and provides personal data of associates during registration without their consent (e.g in <i>Admin</i> and <i>Tech</i> fields) (p. 21)	Liability depending on severity of violation (p. 12)	Obtain consent from relevant associates to share personal data as part of registration OR provide generic contact information (e.g. <i>admin@company.example</i>) (p. 28)	Improves reachability [neutral value assigned as some legal person registrants do not want their data publicly available in RDDS] (p. 24)	-1
RDDS End-Users	May inadvertently process personal data as a result of incorrect self-identification (p. 20)	Liability depending on severity of violation (p. 12)	Apply technical methods to identify and remove personal data from any RDDS data obtained [neutral value assigned as these methods impose costs] (p. 45)	More RDDS data available as a result of RDDS data differentiation (p. 42)	-1

Scenario 1 (Registrant Self-Identification): Feasibility Value by Party

$$[\text{Risk } (-R) + \text{Cost } (-C)] + [\text{Mitigation } (M) + \text{Benefits } (B)] = \text{Feasibility Value } (FV)$$



Contracted Parties



Risk = -1

FV = - 2

Cost = -1

$$(-R + -C) + (M + B) = FV$$

Mitigation = 0

$$(-1 + -1) + (0 + 0) = - 2$$

Benefits = 0



Natural Person Registrants



Risk = -1

FV = - 2

Cost = -1

$$(-R + -C) + (M + B) = FV$$

Mitigation = 0

$$(-1 + -1) + (0 + 0) = - 2$$

Benefits = 0



Legal Person Registrants



Risk = -1

FV = - 1

Cost = -1

$$(-R + -C) + (M + B) = FV$$

Mitigation = 1

$$(-1 + -1) + (1 + 0) = - 1$$

Benefits = 0



RDDS End-Users



Risk = -1

FV = - 1

Cost = -1

$$(-R + -C) + (M + B) = FV$$

Mitigation = 0

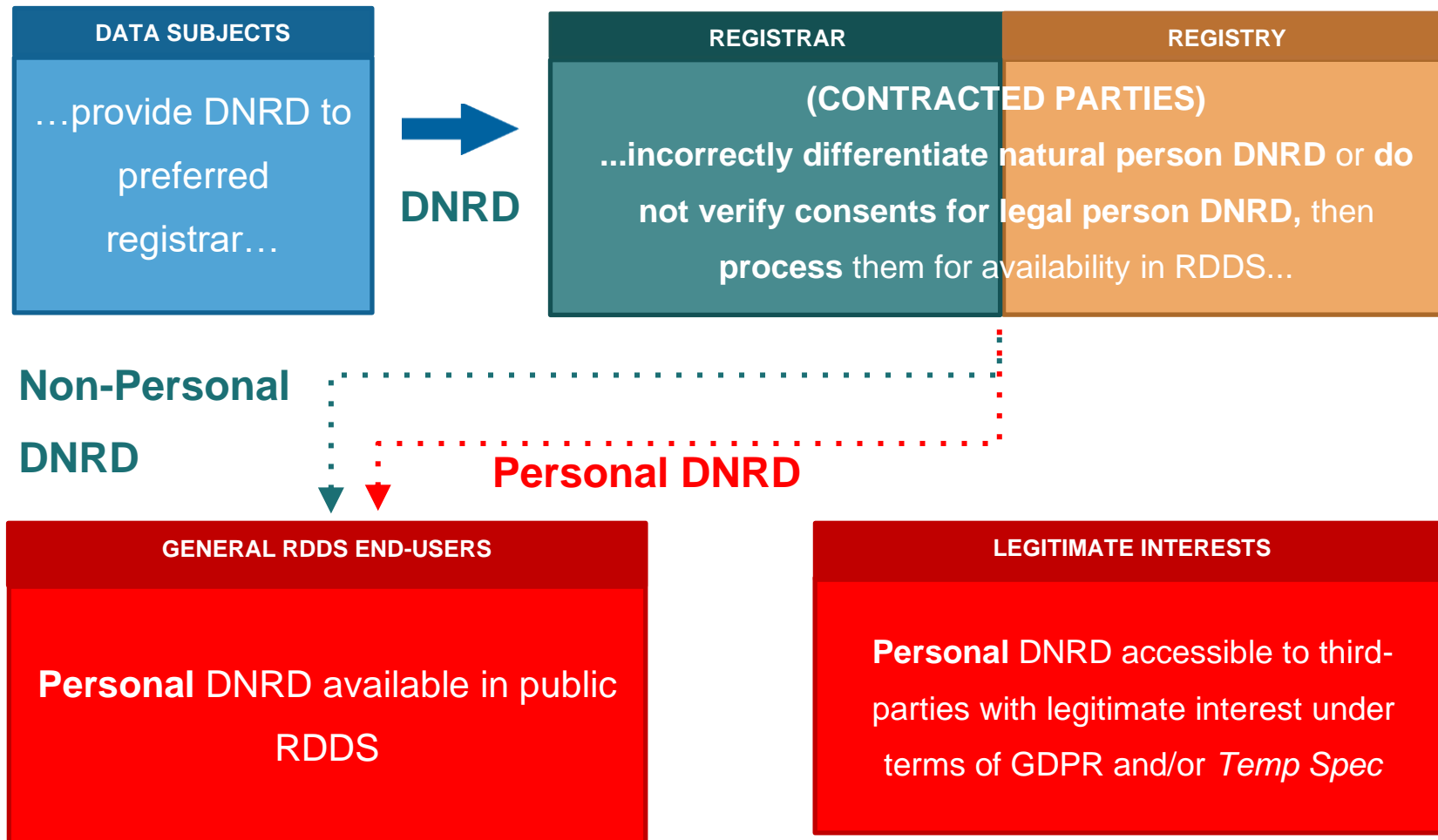
$$(-1 + -1) + (0 + 1) = - 1$$

Benefits = 1

Scenario 2: Differentiation by Contracted Party

Scenario 2: Differentiation by Contracted Party Problem Map

The following process map illustrates a scenario in which a registrant provides personal data, i.e. as a natural person registrant OR as a legal person registrant on behalf of associates *without* their consent:



Scenario 2 (Differentiation by Contracted Party): Feasibility Assessment Heat Map

$$[\text{Risk } (-R) + \text{Cost } (-C)] + [\text{Mitigation } (M) + \text{Benefits } (B)] = \text{Feasibility Value } (FV)$$

	Risks	Costs	Mitigation	Benefits	FV
Contracted Parties	Misidentify natural person registrant as legal person registrant; personal RDDS data flagged for availability in public RDDS (p. 21)	Liability depending on severity of violation (p. 12)	Verify designation [neutral value assigned as verification is a cost as well as mitigation measure] (p. 31)	N/A compared to <i>Scenario 0</i>	-2
Natural Person Registrants	Misidentified by Contracted Party as a legal person registrant; personal RDDS data flagged for availability in public RDDS (p. 21)	Privacy (p. 23)	N/A	N/A	-2
Legal Person Registrants	Personal data of associates processed without proper consent (e.g. in <i>Admin</i> and <i>Tech</i> fields) (p. 21)	Liability depending on severity of violation (p. 12)	Obtain consent from relevant associates to share personal data as part of registration OR provide generic contact information (e.g. <i>admin@company.example</i>) (p. 28)	Improves reachability [neutral value assigned as some legal person registrants do not want their data publicly available in RDDS] (p. 24)	-1
RDDS End-Users	May inadvertently process personal data as a result of incorrect designation; or personal data are included in legal person DNRD without proper consent (p. 20 and p. 21)	Liability depending on severity of violation (p. 12)	Apply technical methods to identify and remove personal data from any RDDS data obtained [neutral value assigned as these methods impose costs] (p. 45)	More RDDS data available as a result of RDDS data differentiation (p. 42)	-1

Scenario 2 (Differentiation by Contracted Party): Feasibility Value by Party

$$[\text{Risk } (-R) + \text{Cost } (-C)] + [\text{Mitigation } (M) + \text{Benefits } (B)] = \text{Feasibility Value } (FV)$$



Contracted Parties



Risk = -1

FV = - 2

Cost = -1

$$(-R + -C) + (M + B) = FV$$

Mitigation = 0

$$(-1 + -1) + (0 + 0) = - 2$$

Benefits = 0



Natural Person Registrants



Risk = -1

FV = - 2

Cost = -1

$$(-R + -C) + (M + B) = FV$$

Mitigation = 0

$$(-1 + -1) + (0 + 0) = - 2$$

Benefits = 0



Legal Person Registrants



Risk = -1

FV = - 1

Cost = -1

$$(-R + -C) + (M + B) = FV$$

Mitigation = 1

$$(-1 + -1) + (1 + 0) = - 1$$

Benefits = 0



RDDS End-Users



Risk = -1

FV = - 1

Cost = -1

$$(-R + -C) + (M + B) = FV$$

Mitigation = 0

$$(-1 + -1) + (0 + 1) = - 1$$

Benefits = 1

Conclusion

The model above provides a simple framework to compare the **risks, costs, mitigation measures, and benefits** associated with differentiation among Contracted Parties, registrants, and RDDS end-users. It illustrates how differentiation—or lack of it—distributes burdens and benefits unequally among these groups. As indicated in the questionnaire, a number of Contracted Parties operating outside the framework of the GDPR said they did not differentiate simply because no law or policy required them to do so. Creating a global policy on differentiation may impose costs and risks on those parties not bound by the GDPR or similar data protection legislation. It may also impose costs and risks on legal and natural person registrants, and even RDDS end-users should they end up processing personal data entered into RDDS without the proper consent.

An ideal differentiation mechanism would maximize the availability of non-personal registration data in RDDS, while minimizing the risks of mis-handling the data of natural persons and the costs of implementing an accurate, reliable method to differentiate. In its resolution adopting the *Temporary Specification for gTLD Registration Data*—the precursor to the *Interim Policy*—the ICANN Board stated part of its rationale for doing so: “to ensure continued availability of the WHOIS service to the greatest extent possible and other processing of gTLD registration data while complying with the GDPR and avoid fragmentation of WHOIS.”¹¹⁴ The EPDP Team echoes this goal in its Charter, stating: “The EPDP Team is being chartered to determine if the *Temporary Specification for gTLD Registration Data* should become an ICANN Consensus Policy, as is or with modifications, while complying with the GDPR and other relevant privacy and data protection law.”

As the GDPR only applies to personal data, differentiation between personal and non-personal data in RDDS could maximize the availability of registration data to serve this end. However, given the imbalance of burden and benefit of differentiation as a practical matter, as well as the likelihood of error given the scale at which these parties operate, it is unlikely that a global policy to differentiate could ever reach a state that each viewed as

¹¹⁴ ICANN Board (17 May 2018), “Consideration of the Temporary Specification for gTLD Registration Data (Implementation of GDPR Interim Compliance Model)”, <https://www.icann.org/resources/board-material/resolutions-2018-05-17-en>, Resolutions 2018.05.17.01 – 2018.05.17.09

“ideal”; whatever the “differentiation scenario”, some party will bear relatively more risk and cost than others, while others will enjoy relatively more benefit.

As illustrated in this report, differentiation is a complex topic with many layers of nuance and potential impact. The information and analysis provided in herein are not presented as definitive or exhaustive. It remains for the EPDP Phase 2 Team to determine the relative merits of differentiation as a policy matter.

References

Adriano, Elvia Arcelia Quintana. 2015. "The Natural Person, Legal Entity or Juridical Person and Juridical Personality." *Penn State Journal of Law & International Affairs* 4 (1): 363 - 391. *Northwestern University Law Review*, <https://elibrary.law.psu.edu/jlia/vol4/iss1/17>

Article 29 Data Protection Working Party (10 April 2018), *Guidelines on Transparency under Regulation 2016/679*, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

Bradford, Anu (2012), "The Brussels Effect", *Northwestern University Law Review*, 107(1), https://scholarship.law.columbia.edu/faculty_scholarship/271

Bird & Bird LLP (25 January 2019), "Memorandum to ICANN org and EPDP Team: Advice on liability in connection with a registrant's self-identification as a natural or non-natural person pursuant to the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') EPDP Wiki: Legal Memos and Input: Natural vs. Legal Memo.docx. <https://community.icann.org/display/EOTSFGDR/EPDP+Small+meeting+on+Legal+Committee+Framework>.

businessextra.com, "Real value for companies with air travel, <https://www.businessextra.com/home.htm>

"Charter for the Temporary Specification for gTLD Registration Data EPDP Team." (19 July 2018), chase.com, "Choose what's right for your business," <https://www.chase.com/business>

Deloitte (2019), "After the dust settles: How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on", <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-the-impact-of-gdpr-on-the-financial-services.pdf>

delta.com, "The No-Cost, Simple Way to Maximize Your Company's Travel Budget," <https://skybonus.delta.com/content/skybonus/corporate/us/en/home.html>

.dk Hostmaster, "Danish Act on Internet Domains," <https://www.dk-hostmaster.dk/en/danish-act-internet-domains>

.dk Hostmaster, "Whois and GDPR," <https://www.dk-hostmaster.dk/en/gdpr>

Economist (20 Feb 2020), "The EU wants to set the rules for the world of technology", <https://www.economist.com/business/2020/02/20/the-eu-wants-to-set-the-rules-for-the-world-of-technology>

Economist (5 May 2017), “The world’s most valuable resource is no longer oil, but data”, <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>

Economist (6 May 2017), “Data is giving rise to a new economy”, <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy>

enforcementtracker.com, “Fines Database,” <https://www.enforcementtracker.com/?insights>.

enforcementtracker.com, “Fines Models by DPAs,” <https://www.enforcementtracker.com/?insights>.

enforcementtracker.com, “Fines Statistics: Highest fines: individual,” <https://www.enforcementtracker.com/?insights>.

enterprise.com, “Car Rental Program for Small and Medium Sized Businesses,” https://www.enterprise.com/en/business-car-rental.html?icid=header.business.solutions-_-business.rental

EURID.eu, “WHOIS Policy,” https://eurid.eu/d/205797/whois_policy_en.pdf

everstring.com, “Contacts - EverString Overview Demo,” <https://vimeo.com/357684590>

everstring.com, “Privacy Policy”, <https://www.everstring.com/privacy-policy/>

Federal Trade Commission (22 November 2019), “YouTube channel owners: Is your content directed to children?”, <https://www.ftc.gov/news-events/blogs/business-blog/2019/11/youtube-channel-owners-your-content-directed-children>

Federal Trade Commission, “Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business”, <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>

gdpr.eu, “How to conduct a Data Protection Impact Assessment”, <https://gdpr.eu/data-protection-impact-assessment-template/>

gdpr.eu, “What are the GDPR Fines?”, <https://gdpr.eu/fines/>

gdpr.eu, “What is GDPR, the EU’s new data protection law?”, <https://gdpr.eu/what-is-gdpr/>

gdpr-info.eu, “GDPR Key Issues: Consent”, <https://gdpr-info.eu/issues/consent/>

General Data Protection Regulation (Regulation 2016/679 of the European Parliament and Council) (27 April 2016), <https://gdpr.eu/tag/gdpr/>

General Data Protection Regulation (27 April 2016), “Art. 35 GDPR: Data protection impact assessment,” <https://gdpr.eu/article-35-impact-assessment/>

General Data Protection Regulation (27 April 2016), “Art. 6 GDPR: Lawfulness of processing”, <https://gdpr-info.eu/art-6-gdpr/>

Google.com, “Frequently Asked Questions about Google Accounts & Age Requirements”, <https://support.google.com/accounts/answer/1333913>

Huffington Post (21 September 2017), “The Surprising Truth About Why Alcohol Websites Make You Enter Your Age”, https://www.huffpost.com/entry/liquor-website-age-verification_n_59c3b549e4b06f93538cdd18

ICANN Board (17 May 2018), “Consideration of the Temporary Specification for gTLD Registration Data (Implementation of GDPR Interim Compliance Model)”, <https://www.icann.org/resources/board-material/resolutions-2018-05-17-en>, Resolutions 2018.05.17.01 – 2018.05.17.09

ICANN GAC (20 February 2019), *Governmental Advisory Committee¹ Input on the Draft Final Report of the Expedited Policy Development Process (EPDP) on gTLD Registration Data*, <https://gac.icann.org/publications/public/epdp-draft+final-report-revised+gac-input-20feb19-final.pdf>

ICANN GNSO (20 February 2019), *Final Report on the Temporary Specification for gTLD Registration Data Expedited Policy Development Process*, <https://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf>

ICANN GNSO (7 February 2020), *Initial Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process*, <https://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-initial-report-07feb20-en.pdf>

ICANN GNSO, “Charter for the Temporary Specification for gTLD Registration Data EPDP Team” (19 July 2018), <https://gns0.icann.org/sites/default/files/file/field-file-attach/temp-spec-gtld-rd-epdp-19jul18-en.pdf>

ICANN.org (2 November 2019), “GNSO - EPDP Phase 2 Meeting (1 of 4)”, <https://66.schedule.icann.org/meetings/1116817>

ICANN.org (25 May 2018), *Temporary Specification for gTLD Registration Data*, <https://www.icann.org/resources/pages/gtld-registration-data-specs-en>

ICANN.org, “Registration Data Policy for gTLDs (EPDP Phase 1 Implementation),” <https://www.icann.org/resources/pages/registration-data-policy-gtlds-epdp-1-2019-07-30-en>

ICANN.org, “WHOIS Accuracy Reporting System (ARS) Project Information,” <https://whois.icann.org/en/whoisars>

ICANN.org, *Interim Registration Data Policy for All gTLDs*, <https://www.icann.org/resources/pages/interim-registration-data-policy-en>

ICANN.org, “Registration Data Policy for gTLDs (EPDP Phase 1 Implementation),” <https://www.icann.org/resources/pages/registration-data-policy-gtlds-epdp-1-2019-07-30-en>

IETF (October 1985), “RFC 954: NICNAME/WHOIS,” <https://www.ietf.org/rfc/rfc954.txt>

Independent (31 January 2019), “Social Media Being Used By Growing Number Of Children Under 11 Despite Age Limits”, <https://www.independent.co.uk/life-style/children-social-media-use-age-limit-facebook-instagram-profiles-a8756096.html>

Jelinek, Andrea (5 July 2018), “Letter from Andrea Jelinek, Chairperson, European Data Protection Board Chairperson, to Goran Marby, ICANN Org CEO”, <https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf>

Kuner, Christopher (2003), “Chapter 2: Fundamental Legal Concepts” in *European Data Privacy Law and Online Business*, (Oxford University Press), pp. 49-84.

Leggett, Theo (12 January 2017), “VW papers shed light on emissions scandal”, *bbc.com*, <https://www.bbc.com/news/business-38603723>

legislation.gov.uk, Data Protection Act 2018, <http://www.legislation.gov.uk/ukpga/2018/12/section/122/enacted>

Marketing Eye (19 December 2017), “GDPR: B2B vs B2C – can you still email your database?”, <https://www.themarketingeye.com/blog/gdpr-b2b-vs-b2c-can-you-still-email-your-database/>

Massachusetts Institute of Technology, Computer Science and Artificial Intelligence Laboratory (2 February 2009), “Transparent Accountable Datamining Initiative”, <http://dig.csail.mit.edu/TAMI/>

Murphy, Kevin (25 May 2018), "How all 33 European ccTLDs are handling GDPR." *DomainIncite*, <http://domainincite.com/23053-how-all-33-european-cctlds-are-handling-gdpr>

Oates, Wallace, Joe Oppenheimer, and Thomas C. Schelling. "In Memoriam: Remembering Mancur Olson." *Southern Economic Journal* 66, no. 3 (2000): 793-800, www.jstor.org/stable/1061440.

Olejnik, Lukasz (2 January 2018), "How to: GDPR, consent and data processing", <https://blog.lukaszolejnik.com/how-to-gdpr-consent-data-processing/>

Olson, Mancur (1971), *The Logic of Collective Action: Public Goods and the Theory of Groups*, Cambridge: Harvard University Press.

orbis.hr, "Register Domain", <https://www.orbis.hr/portal/cart.php?a=confdomains>

Ramnath Chellappa, Ravinder Dharmapuram, and Rahul Hampole (22 April 2006), "Dynamic Privacy Enforcer: A Trusted Third-party Framework to Provide Personalization in the Presence of Privacy Concerns", *Proceedings of the CHI2006 Workshop on Privacy-Enhanced Personalization*, Montreal, <http://isr.uci.edu/pep06/program.html>, pp. 16 - 20.

Rėklaitis, Kėstutis & Pilelienė, Lina. (2019). Principle Differences between B2B and B2C Marketing Communication Processes. *Management of Organizations: Systematic Research*. 81. 73-86. <https://content.sciendo.com/view/journals/mosr/81/1/article-p73.xml?language=en>

RIPE Labs (1 February 2018), "How We're Implementing the GDPR: The RIPE Database", <https://labs.ripe.net/Members/Athina/how-we-re-implementing-the-gdpr-the-ripe-database>

RIPE Labs (6 March 2018), "How We're Implementing the GDPR: Legal Grounds for Lawful Personal Data Processing and the RIPE Database", <https://labs.ripe.net/Members/Athina/gdpr-legal-grounds-for-lawful-personal-data-processing-and-the-ripe-database>

Security and Stability Advisory Committee (14 June 2018), *SAC 101: SSAC Advisory Regarding Access to Domain Name Registration Data*, <https://www.icann.org/en/system/files/files/sac-101-en.pdf>

Sonovate, "Key differences between B2B and B2C when it comes to GDPR", <https://www.sonovate.com/blog/key-differences-b2b-b2c-gdpr/>

United Kingdom's Information Commissioner's Office (UK ICO), "The rules around business to business marketing, the GDPR and PECR", <https://ico.org.uk/for-organisations/in-your-sector/marketing/the-rules-around-business-to-business-marketing-the-gdpr-and-pecr/>

UK ICO, "When can we rely on legitimate interests?", <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/>

UK ICO, (9 February 2018), "Sample DPIA Template", <https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf>

UK ICO, "Principle (d): Accuracy," <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>

United States Justice Department (14 January 2015), *Prosecuting Computer Crimes*, <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>

Van Evera, Stephen (1997), *Guide to Methods for Students of Political Science*, Cornell University Press.

w3.org (2 February 2018), "Platform for Privacy Preferences (P3P) Project", <https://www.w3.org/P3P/Overview.html>

Weitzner, Daniel J., Jim Hendler, Tim Berners-Lee and Dan Connolly (2006), "Creating a Policy-Aware Web: Discretionary, Rule-Based Access for the World Wide Web" in *Web and Information Security*, eds. Elena Ferrari and Bhavani Thuraisingham, pp. 1 - 31.